


 National Indian Gaming Commission


CJIS

A Primer for Compliance




 Training Objectives

- MOU between the NIGC and FBI
- LASO requirements
- KE / PMO Classification Guide
- Outsourcing Agreements
- First Steps to Achieve Compliance


 NIGC & FBI MOU

- KE / PMO
- Authority & Purpose for CJ / CHRI
- Sanctions/Penalties

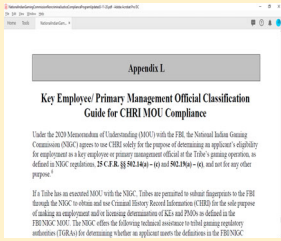



 **LASO Requirements**



 **KE/PMO Classification Guide**

This guide or similar process should be used by TGRA



 **Outsourcing Agreements**

Required by the National Crime Prevention and Privacy Compact Council

- When a contractor performs a non-criminal justice administrative function.
- Outsourcing includes Casino or Tribal IT personnel

Outsourcing Agreement Process

- Prepare draft contract with contractor / vendor
- Send letter and draft contract to FBI Compact Officer (& a copy to the NIGC ISO)
- Once approved, execute contract and audit contractor within 90 days

First Steps to Achieve Compliance

- Review MOU
- Update & Submit Authorized Personnel List
- Complete Security Awareness Training

First Steps to Achieve Compliance

- Review resource information
- Complete CJIS IT Questionnaire
- Develop / Refine TGRA policies

First Steps to Achieve Compliance

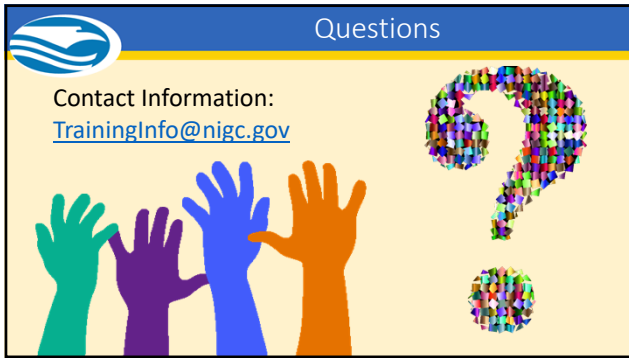
- Complete TGRA policy training
- Acknowledgement Statement
- Outsourcing Agreements

First Steps to Achieve Compliance

- Prepare for first NIGC audit
- Internal auditing / monitoring
- Complete training cycles

NIGC Resources

- Updated Website
<https://www.nigc.gov/compliance/CJIS-Training-Materials>
- Upcoming Regional Training Conferences



Questions

Contact Information:
TrainingInfo@nigc.gov

The graphic features the National Indian Gaming Commission logo in the top left corner. Below it, the text 'Questions' is centered at the top. Underneath, the contact information 'Contact Information: TrainingInfo@nigc.gov' is displayed. The bottom half of the graphic shows four stylized hands in green, purple, blue, and orange, with a large question mark composed of colorful mosaic tiles to their right.

National Indian Gaming Commission Noncriminal Justice Compliance Program



Noncriminal Justice Agency Guide for Federal Criminal History Checks

Document Updated: March 11, 2020

Table of Contents

Introduction	5
Contact List	6
Section 1 General Overview	
1.1 NIGC Overview	7
1.2 Memorandum of Understanding	7
1.3 Authorizations and Access	8
1.3.1 Application for Access	8
1.3.2 Noncriminal Justice Access	8
1.4 Outsourcing Agreements	9
1.4.1 Outsourcing Agreement Submission	9
1.4.2 Contract Regarding Outsourcing Noncriminal Justice Functions	9
Section 2 Fingerprint Submissions & Results	
2.1 NIGC Fingerprinting Process	11
2.1.1 Fingerprint Criminal History Check Process	11
2.2 Applicant Identification	11
2.3 FBI Applicant Privacy Rights Notifications and Privacy Act	12
2.4 Electronic (Live Scan) Fingerprint Submission System Connectivity	12
2.5 Mail Reply(s)	13
2.6 System Testing	13
2.7 Step by Step Transaction Flow(s)	13
2.8 Basic Hard Card Fingerprinting Tips	15
2.9 Protection of the Fingerprint Card Prior to Submission	17
2.10 Required Information for Each Fingerprint Card Submission	17
2.10.1 Fingerprint Card Legend	17
2.11 Example Fingerprint Card	20
2.12 Payment and Submission Packets	20
2.12.1 Fees	20
2.12.2 Payment Submittal Requirements	21
2.13 Rejected Fingerprint Cards/Resubmissions	21
2.13.1 Routine Name Search Procedure	21
2.13.2 Example Individual FBI Reject Notice	22
2.14 Example FBI Criminal History Record	23
Section 3 Basic Privacy & Security Guidelines	
3.1 Policies and Procedures	34
3.2 Applicant Process	35
3.3 Applicant Review and Challenge of Criminal History	35
3.4 Communication/Dissemination	36
3.4.1 Communication Cautions	36
3.4.2 Secondary Dissemination	37
3.5 Physical Security	37
3.5.1 Storage	37
3.5.2 Destruction	38

3.6	Technical/Digital Security	38
3.7	Consequences for Misuse	39
Section 4 LASO Responsibilities		
4.1	Primary Liaison	41
4.1.1	Information Changes	41
4.1.2	Authorized Personnel List	42
4.2	Privacy and Security Coordinator	42
4.2.1	Required Training for Authorized Personnel	42
4.2.2	Acknowledgement Statements	43
4.3	Audit Responsibilities	43
Section 5 Audits & Compliance		
5.1	Audits	44
5.1.1	Routine Audits	44
5.1.2	Directed Audits	44
5.2	Compliance Review	45
5.2.1	General Administration	45
5.2.2	Fingerprint Submissions	46
5.2.3	Privacy and Security	47
5.2.4	Training	48
5.2.5	Key Employee and Primary Management Official Checklist	48
5.2.6	Gaming Operation Definition	48
5.2.7	Key Employee Definition	48
5.2.8	Primary Management Definition	49
5.3	National Identity Services Audit	49
5.4	Information Technology Security Audit	50
5.4.1	Noncriminal Justice Audit	50
5.4.2	Outsourcing/Channeling Audit	50
Section 6 NIGC Classes & Assistance		
6.1	Initial Access & NCJA Compliance Training	51
6.2	Types of Training Offered by the NIGC	51
6.3	Requesting Site Specific Training from the NIGC	51
6.4	Other Training Options	52
Section 7 First Steps to Achieve Compliance		
7.1	How to Achieve Compliance	53
References		55
Acronym Glossary		56
Appendix A	Memorandum of Understanding	57
Appendix B	Select Pages from the FBI Outsourcing Standards	60
Appendix C	FBI Required Privacy Act and Noncriminal Justice Applicants Rights Notice	78
Appendix D	NIGC Fingerprint System Security, Protocols and Data Requirements	80
Appendix E	CJIS Name Search Request Form	85
Appendix F	Sample Policies for CHRI Access, Use, Handling and Dissemination	86
Appendix G	LASO Responsibilities Handout	127
Appendix H	Sample Noncriminal Justice Agency Information Change Form	128
Appendix I	Sample Authorized Personnel List	129

Appendix J	Sample Training Documentation Form	130
Appendix K	NIGC Fingerprint MOU/CJIS Checklist and IT Security Audit Checklist	131
Appendix L	Key Employee and Primary Management Official Checklist	155
Appendix M	Bulletin – Fingerprint processing – Applicant Privacy Act rights and protecting CHRI	159
Appendix N	Sample Notice of Results	163

Introduction

The purpose of this guide is to assist federally recognized gaming tribes and their tribal gaming regulatory authorities (TGRA) in successfully submitting fingerprints to the National Indian Gaming Commission (NIGC). Pursuant to the Indian Gaming Regulatory Act (IGRA) and NIGC regulations, the NIGC processes fingerprints for persons at the tribes' gaming enterprises who come within the statutory and regulatory definitions of key employees and primary management officials. From the NIGC, tribes receive criminal justice information (CJI) and criminal history record information (CHRI) for noncriminal justice purposes pursuant to authorizations under federal law.¹ CJI refers to all of the FBI Criminal Justice Information Services (CJIS) provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to, biometric, identity history, biographic, property, and case/incident history data. CHRI means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, information, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, and release. CHRI is also information transferred or reproduced directly from CHRI, information that confirms the existence/ nonexistence of CHRI, letters, emails, documents, notes, conversations in person/phone, and databases including spreadsheets or tables.

Public Law 92-544, passed by Congress in October 1972, authorizes the FBI to exchange CHRI with officials of governmental agencies for noncriminal justice purposes (i.e., for licensing and employment). In 1998, the National Crime Prevention and Privacy Compact Act was passed allowing signatory states to exchange criminal history records for noncriminal justice purposes according to a uniform standard. The 1998 act also established the National Crime Prevention and Privacy Compact Council to regulate and assist in maintaining a method of exchange of CHRI, which protects both public safety and individual privacy rights. The FBI Criminal Justice Information Services (CJIS) Division houses the largest repository of fingerprint criminal history records and is responsible for overseeing the exchange of such records. Federal laws, regulations, and policies govern the release of information exchanged through the FBI and require states to regulate access, use, quality, and dissemination of state-held records.

Both state and federal criminal justice and CHRI is subject to laws, rules, and regulations governing its access, use, handling, and dissemination. This guide assists tribes and their noncriminal justice agencies with proper fingerprint submittals, provides guidance regarding agencies' responsibilities for appropriate information handling, informs agencies of requirements associated with the use of the state and federal criminal history check processes, as well as training offered by the NIGC. Additionally, it discusses the two sets of rules you will hear often is National Identity Systems requirements and CJIS Security Policy.

¹ 25 U.S.C. §§ 2706(b)(3), 2706(b)(7), 2706(b) (10), 2708, 2710(b)(2)(F), 2710(c)(1)-(2), 2710(d)(9), 2711(a), 2711(e), and 28 U.S.C. § 534.

National Indian Gaming Commission Contact List

Fingerprint Assistance

NIGC Investigative Programs Specialist

Available Monday through Friday from 8 a.m. to 5 p.m. Closed on Federal Holidays.

NIGC Investigative Programs Specialist – Mr. Seneca Chavis

Email: fingerprint_admin@nigc.gov

Phone: (202) 632-7003

Fax: (202) 632-7066

Physical Address:

National Indian Gaming Commission
90 K Street NE, Suite 200
Washington, DC 20002

Mailing Address:

National Indian Gaming Commission
1849 C Street NW
Mail Stop #1621
Washington, DC 20240

Technical Assistance

National Indian Gaming Commission Technical Support

Available Monday through Friday from 8 a.m. to 5 p.m. Closed on Federal Holidays.

NIGC Information Security Officer

Email: iso@nigc.gov

Phone: 202-632-7003

Fingerprint Billing/Invoices

Email: Fingerprint_Billing@nigc.gov

Phone: 202-632-7003

Section 1 – General Overview

1.1 NIGC Overview

The NIGC is the Central Terminal Agency (CTA) for over 240 federally recognized tribes and their tribal gaming regulatory authorities (TGRA) for purposes of processing their key employee and primary management official applicants' electronic and ten print fingerprint cards through the FBI's IAFIS (Integrated Automated Fingerprint Identification System). The vast majority of the NIGC applicant cards are processed electronically through a NIGC-approved live scan vendor. Tribes without live scan equipment can mail ten print fingerprint cards (AKA hard cards) to the NIGC where the cards are scanned and submitted to the FBI electronically. The FBI then returns the results to NIGC to be shared with the tribe's TGRA for the sole purpose of determining the eligibility of applicants for key employee and primary management official positions in its gaming enterprise(s).

The NIGC system is designed so the NIGC and tribes do not use "FBI-approved Channelers". Channelers push and pull both CHRI and personally identifiable information (PII)/fingerprints. The NIGC and tribes use "NIGC approved live scan vendors" to simply push PII/fingerprints to NIGC and the NIGC pushes the CHRI data it receives from the FBI to the tribes. Some of the NIGC approved live scan vendors are also FBI-approved Channelers, but it is not a requirement. There is sometimes confusion about the two designations. For a list of NIGC approved live scan vendors please visit <https://www.nigc.gov/finance/fingerprint-process>. If you do not find your vendor on the list, please contact the NIGC Investigative Programs Specialist at fingerprint_admin@nigc.gov to confirm their status.

Under the CJIS Security Policy, the NIGC is required to designate a CJIS Systems Officer (CSO) to ensure that CHRI data is handled and stored properly at NIGC and at the tribes' locations. The CSO responsibilities include:

- Monitoring the NIGC and TGRAs' locations and systems to ensure system maintenance and records security, and
- Ensuring proper dissemination of CJI, including CHRI.

Established policies, procedures, and standards must be strictly adhered to in order to maintain the integrity of the system and its records. With respect to compliance with the federal regulations for system access and maintenance, the NIGC performs several duties:

- Conducting audits of the use and dissemination of CHRI and criminal history records,
- Training concerning use of system information, and
- Monitoring system access and researching/investigating security breaches.

1.2 Memorandum of Understanding

As the Central Terminal Agency (CTA) between the FBI and the Tribes, the NIGC entered into an updated Memorandum of Understanding (MOU) with the FBI on January 17, 2020. The MOU documents the agreed-upon responsibilities and function of the FBI and NIGC with respect to the submission of noncriminal fingerprints for primary management officials and key employees of Indian gaming enterprises, as defined by NIGC regulations, 25 C.F.R. §§ 502.14 (a-c) and 502.19 (a-c). For more information, see the NIGC and FBI MOU in Appendix A and Section 5.2 which covers the definitions of gaming operation, key employee and primary management official.

Each Tribe authorized to receive CJI and CHRI must sign a MOU with the NIGC. The MOU is a contractual agreement between the Tribe and NIGC. It must be signed by both an NIGC representative and the appropriate tribal official.

A sample of the current NIGC/Tribal MOU can be found in Appendix A. NIGC is developing a new NIGC/Tribal MOU in 2020 that all tribes must sign on or before January 1, 2021. The new NIGC/Tribal MOU will contain the following terms and conditions:

- Authority and Purpose: The MOU states the nature of the requesting organization, the purpose for which CJI and/or CHRI is requested, and the specific authorization granting access to the information. **It is prohibited for noncriminal justice agencies to use CJI and CHRI for any purpose other than that for which it was requested.**
- Sanctions/Penalties: The NIGC agrees to promptly notify tribal authorities if it determines that it is necessary to discontinue disseminating CHRI to the tribe (either in whole or in part) due to the tribe's failure to comply with conditions set forth in the MOU.
- Local Agency Security Officer: The new MOU requires the appointment of a Local Agency Security Officer (LASO) to act as liaison with the NIGC. (Section 4 of this guide covers the responsibilities of the LASO).
- Training: TGRAs are responsible for mandatory training requirements. TGRAs opening a fingerprint access for the first time must complete the Initial Access & NCJA Compliance Training prior to submitting fingerprint cards. For existing TGRAs, all tribal personnel who view or handle CHRI must complete the standard online training (currently called CJIS Online) and undergo tribal internal training on CHRI security and handling based on the required policies/procedures.
- Policies/Procedures: As part of privacy and security, TGRAs must implement policies and procedures that provide for the security and proper handling of the CJI/CHRI. TGRAs must also have rules for fingerprint submissions that include proper applicant identification and protecting fingerprint cards from tampering.

1.3 Authorizations and Access

Before access to the fingerprint system may be granted to a tribe, the tribe must contact the NIGC and request a pre-activation package. The packet includes a cover letter, systems requirements and a system checklist.

1.3.1 Application for Access

Prior to submitting fingerprint cards and receiving CHRI, a tribe must complete a pre-activation packet, sign the NIGC/Tribal MOU and complete Initial Access & NCJA Compliance Training.

The training is designed to assist the tribe in carrying out its responsibilities under the MOU and maintaining compliance with laws and regulations. Once initial requirements are met, the NIGC will schedule activation and testing and the tribe is issued an Originating Case Agency number (OCA), which is a nine-character alphanumeric identifier. This number is the tribe's submission access number for fingerprint criminal history record checks. All submissions are made under the NIGC's ORI number which will be provided upon activation.

1.3.2 Noncriminal Justice Access

Use of CHRI obtained from noncriminal justice fingerprints is strictly limited to the noncriminal justice purpose (licensing or employment) and **may not** be shared for criminal justice or any other purposes. Do not disseminate any forms of CHRI to anyone or any entity not directly involved in the licensing process at the Tribe and NIGC. The Tribe cannot duplicate, disseminate, or re-use CHRI, including sharing it with applicant's spouse, household, other family members, tribal leadership, other tribal agencies not involved in licensing key employees or primary management officials, human resource departments, other potential employers, and state gaming or licensing agencies. To be clear, even if the use of CHRI may be necessary to satisfy state licensing requirements, CHRI from NIGC cannot be used for such purpose – a new record request

to the FBI through a non-NIGC process must be made in such instances.

1.4 Outsourcing Agreements

In accordance with the National Crime Prevention and Privacy Compact (Compact) Council's Final Rule entitled "Outsourcing of Noncriminal Justice Administrative Functions" (28 C.F.R. part 906), outsourcing of noncriminal justice administrative functions is permitted under certain conditions when approved by the FBI Compact Officer and as specified in the Security and Management Control Outsourcing Standard for Non-Channelers (Outsourcing Standard) located at <https://www.nigc.gov/compliance/CJIS-Training-Materials>.

1.4.1 Outsourcing Agreement Submission

Non-channeler Outsourcing Agreements are required when a TGRA uses an entity, contractor or vendor to assist it with handling, storing, or moving electronic or physical CJI or CHRI. To ensure compliance with the standard, if the TGRA uses a third party, including the casino's or tribe's Information Technology (IT) department, to maintain the network, servers or computers which access and store CHRI, an outsourcing agreement must be drafted and submitted to the FBI Compact Officer for approval prior to executing the agreement and engaging the service.

To contract noncriminal justice administrative functions to a third party, the TGRA must submit a letter requesting approval to use the entity, contractor, or vendor to the FBI Compact Officer, copying the NIGC CSO at iso@nigc.gov. The letter is standard format and a sample can be found in Appendix B.

Additionally, a draft, unexecuted contract between the TGRA and the contractor must accompany the request letter. A sample contract can be found in Appendix B.

1.4.2 Contract Regarding Outsourcing Noncriminal Justice Functions

The contract is standard format and details the parties, what functions are to be outsourced, and the requirement for all CJI and personal identifying information (PII) to be returned to the tribe upon termination of the contract. Upon receiving approval from the FBI Compact Officer, the TGRA and contractor can execute the approved draft contract. Additionally, the TGRA must audit the contract and contractor within 90 days of its execution and certify compliance to the FBI Compact Officer. A sample audit can be found in Appendix B.

Examples of when Outsourcing Agreements are needed:

Shredding: If a TGRA wants to employ a shredding company to destroy CHRI and/or summary CHRI at the TGRA location or are allowed to leave with the documents, an approved outsourcing contract is required.

Storage: If the Tribe uses an off-site storage facility for document storage including CHRI or summary CHRI and storage facility employees have access to CHRI in the box or the facility employees store the CHRI in a locked container that they control, an outsourcing contract is required.

Public Telecom Carriers: If the Tribe uses a public telecom service, which has access to servers,

or provide patches to the servers where CHRI is stored, an outsourcing contract is required. If the telecom service does not have access to the servers or provide patches, outsourcing is not required, which is typically the case.

Electronic Media: If a third party stores electronic CHRI data for a tribe an outsourcing contract is required.

Live Scan Vendors : If a NIGC-approved live scan vendor solely provides live scan service to the TGRA and does not have access to CHRI, an outsourcing contract is not needed. However, if the live scan vendor has access to CHRI² or provides services over and above live scan activities, including but not limited to - data storage of CHRI, network maintenance, or licensing applications where CHRI is stored or summary CHRI information is documented - an outsourcing agreement is required.

If the tribe receives and/or stores CHRI results on the same laptop or computer the live scan device is uses to send the fingerprints to NIGC and the live scan vender has, at any point in time, access, escorted or unescorted, to the CHRI information, an outsourcing agreement is required.

If the tribe purchased the laptop from the live scan vender and has a service agreement for the laptop where CHRI results are received and/or stored, an outsourcing agreement is required.

In summary, if any entity, contractor, or vendor has access to electronic summary CHRI data in electronic or hard-copy form, an outsourcing contract is required.

² This includes any indication that a FBI CHRI record exists or does not exist for a given applicant.

Section 2 - Fingerprint Submissions & Results

The information in this section is intended to assist tribes with the following:

- Understanding the fingerprinting process with the NIGC
- Applicant identity verification and fingerprint card tampering prevention
- Complying with FBI applicant privacy notification requirements
- Filling out the fingerprint card properly
- Assembling a fingerprint submission packet
- Interpreting FBI results

2.1 NIGC Fingerprinting Process

There are two fingerprinting processes to obtain CHRI results through the NIGC—electronic fingerprint and hard card fingerprint submissions. The subsections below explain the fingerprint criminal history check process. Please note that this guide concentrates on electronic fingerprint submissions and compliance rules for the fingerprint criminal history check process.

2.1.1 Fingerprint Criminal History Check Process

In the fingerprint criminal history check process, the tribe has a legal authorization via IGRA and NIGC regulations to submit applicant fingerprints to the NIGC. The process takes place between the tribe and the NIGC whereby the tribe submits the prints and the available criminal history record is sent to the tribe for review. If there is no criminal history, the NIGC and/or FBI results report will indicate a negative response. The use of the criminal history results is limited for the sole purpose outlined in IGRA – employment and/or licensing of key employees or primary management officials in the tribe’s gaming enterprise. The Tribe must have an active MOU on file with the NIGC and is subject to compliance regulations and periodic audits.

The fingerprint criminal history check process is a “point in time” check, and a tribe may only see changes to a person’s criminal history if the fingerprints were submitted again. With a fingerprint criminal history check, the tribe sees the actual criminal history and makes the eligibility determination regarding the applicant, not the NIGC. The NIGC may object to the licensing of an applicant based on criminal history or other background investigation findings; however, the final licensing decision is made by the tribe.

2.2 Applicant Identification

Agencies must have quality assurance processes for verifying the identity of the applicant at the time of fingerprinting.

The National Crime Prevention and Privacy Compact Council published the *Identity Verification Program Guide* containing suggestions and best practice recommendations for verifying an applicant's identity and safeguarding the integrity of the fingerprints. A copy of the guide can be downloaded from the FBI website in the Compact Council section at <https://www.fbi.gov/services/cjis/compact-council>. Compact Council recommendations regarding proper identification of applicants include:

Accept only valid, unexpired photo identification documents as primary proof of identity.

- When accepting secondary identification (i.e. birth certificate, Social Security card), ask for supporting documentation such as a utility bill, bank statement, or mortgage documents.
- Use additional identification data support methods such as:
 - Examine the applicant’s photograph on the identification provided and visually compare the picture with the applicant.

- Compare the physical description on the documentation to the applicant's features (e.g. height, weight, hair and eye color, age, etc.)
- Request the applicant to verbally provide date of birth, address, etc. and verify the answers with the identification provided.
- Check the applicant's signature provided in person with a signature on the identification provided.
- Examine the provided identification to ensure that it has not been altered in any manner.

2.3 FBI Applicant Privacy Rights Notice and FBI Privacy Act

Per Title 28 C.F.R. 50.12 (b), whenever a tribe submits fingerprints for FBI criminal history record checks, the following actions/disclosures are required:

- The person being fingerprinted, meaning the applicant, must be:
 - provided a written FBI Privacy Act Statement (dated 2013 or later) when submitting their fingerprints and associated personal information; and
 - notified in writing that the fingerprints will be used to check the criminal history records of the FBI.
- Simply stating that the applicant is subject to a “national background check” is NOT sufficient.
- The applicant must be informed that they are allowed a reasonable time to change, correct, update, complete, and/or challenge the accuracy of their criminal history record. ALL applicants must be advised of this right, not just those who dispute an employment/license denial.
- The applicant must be advised about how to obtain a copy of their FBI criminal history record and the procedures for challenging it or obtaining a change, correction, or update to it as set forth in Title 28 C.F.R. § 16.34. The tribe may provide a copy of the record to the applicant for this purpose, if it has established a written policy to do so.
- The tribe must also establish and document what constitutes a reasonable period of time for a review and challenge to a record and any appeals process that is available to an applicant for such a challenge.
- If the applicant elects to review/challenge the criminal history record, the tribe must provide the applicant a reasonable period of time to do so before making licensing or employment decision.

A copy of the *Noncriminal Justice Applicant's Privacy Rights* and the *FBI Privacy Act Statement* can be found in Appendix C of this guide and at the NIGC website at <https://www.nigc.gov/compliance/CJIS-Training-Materials>. The FBI updates the notices periodically (usually in the June or November), so the Tribe is encouraged to visit the FBI CJIS websites often to ensure current documents are used:

<https://www.fbi.gov/services/cjis/compact-council/privacy-act-statement> and

<https://www.fbi.gov/services/cjis/compact-council/guiding-principles-noncriminal-justice-applicants-privacy-rights>

2.4 Electronic (Live Scan) Fingerprint Submission System Connectivity

The NIGC, using an AltaScan Store and Forward (SnF) system and a Post Office Protocol 3 (POP3) mail server, provides each tribe a network connectivity path to the FBI's IAFIS system. The SnF is capable of receiving ANSI NIST/EFTS 6.2 and EFTS 7.0 compliant submissions for processing to the IAFIS. Additionally, the SnF is capable of receiving electronic FBI results (SRE) and CHRI as well as Ten Print Transaction Errors (ERRT) and returning these to the submitting tribe. The NIGC interface provides an industry standard, open connectivity path for any tribe, using any EFTS compliant system, to connect and submit electronic fingerprint submissions for processing by the FBI. To ensure convenient and open connectivity, the NIGC choose to use the Internet to allow agencies to transmit and receive fingerprint transactions. Therefore, each tribe will need an Internet Service Provider (ISP) to allow their fingerprint submission system (or device) to access the Internet. Because the fingerprint submissions are rather large files (350 Kb to 1 Mb), NIGC recommends the connection speed be at least 56Kbs to maximize submission throughput. Each tribe should scale the provided bandwidth to accommodate expected fingerprint activity.

If a tribe has a firewall, ports 500 and 4500 will need to be open for two-way traffic.

The tribe's fingerprint system must use a strong authentication and encryption process to submit fingerprints electronically. The fingerprint system should also be configured to register for and use group authentication.

The Tribe's fingerprint system should be configured to send the electronic submissions to the NIGC provided Fingerprint Internet Mail Server (SMTP). The 'To' address is provided on the Pre-Activation checklist for initial set up.

The SnF will process the submissions and receive the FBI results. The SnF will then send the FBI result to the tribe's mailbox located on the NIGC Fingerprint Internet Mail Server (POP3). The tribe's fingerprint system should be configured to retrieve their fingerprint results from this mailbox. The FBI's return policy for applicant submissions is 24 hours. However, most responses usually arrive between 20 minutes and 1 day after submission. The Fingerprint Internet Mail Server holds the responses in the mailbox until the tribe connects and retrieves them. The SnF system will also send a copy of the FBI results to the tribe's designated NIGC regional office.

The tribe's fingerprint system should be configured to limit the amount of times VPN connections can be made to the NIGC's VPN in order to retrieve FBI results. The NIGC's VPN gateway services the tribe's access to the NIGC Fingerprint system as well as remote access for NIGC offices and personnel. To ensure all users will have reasonable access to retrieve FBI results in a timely manner and that the VPN gateway resources are not over utilized, the Tribe's fingerprint system should be configured to access the VPN gateway at no less than 15 minute intervals.

For more information on System Security, System Protocols and Data Requirements please see Appendix D.

2.5 Mail Reply(s):

After submissions are successfully sent to the FBI's IAFIS system, results are returned electronically to the NIGC's AltaScan SnF, which, in turn, sends the results to the NIGC Fingerprint Internet Mail Server (POP3) and ultimately to the submitting tribe. In order to correctly send responses back to the submitter, all electronic submissions should have a tribe specific, NIGC issued, return e-mail address in the "from" line of the submission. The NIGC's SnF system dynamically links the "From" address of a submission to the TCN/TCR number(s) of each submission. This allows the submitter end to change without re-configuring the NIGC's systems. Again, the "From" line of the submission is provided in the Pre-Activation Checklist.

The submitting device must be capable of accepting ANSI NIST/EFTS compliant responses as reply messages. These messages must be de-MIME'd and interpreted by the submitter when received. The responses will provide Ident and Non-Ident information. For Ident responses, the FBI will attach the RAP sheet if requested and is available. In order to receive RAP sheets, the submission must have Request for Rap Sheet (2.070) set to 'Y' for Yes.

2.6 System Testing:

Submission testing must be completed before any electronic submitter can go "live." The tribe will send an email to Itsupport@nigc.gov in order to request for a time slot to conduct a test. One of the Itsupport personnel will coordinate the testing date and the account will be converted into a test mode in the NIGC fingerprint system. As soon as the account is in test mode, the tribe submits or transmits a test electronic fingerprint data with a SSN starting with 002-00-0001. The tribe should receive a response from the FBI by logging in into the NIGC fingerprint system. Upon successful completion of the test, the tribe will send an email to Itsupport@nigc.gov requesting that the account will be converted into a production mode.

2.7 Step by Step Transaction flow(s):

After complying with the above sections, a request by the authorized tribal personnel should be submitted to itsupport@nigc.gov for the following: a) Connection parameters to the NIGC fingerprint system ; b) Instructions on the VPN client to install for Windows 10 only; c) If utilizing the Cisco 5.x client, please consult with your fingerprint vendor to obtain the Cisco 5.x client.

The following is a step-by-step transaction flow of a typical submission:

1. An applicant's fingerprint images are scanned by a Scan device (Live Scan or Card Scan) and formatted into an EFTS compliant electronic NIST record. All applicable demographic information is entered and automatically attached (single part) to the ten print scan. The scanner device will format the images and demographics into an EFTS compliant submission. (See your scan device documentation for details).
2. The tribe's submission device will connect to the Internet. The bandwidth of the connection should be sized according to the expected volume bearing in mind that each NIST submission will range in size from 350Kb to 1 Mb. The NIGC recommends at least a 56 Kbps modem connection.
3. Once a connection to the Internet is established, an IPSec connection or L2PT connection to the NIGC firewall (VPN gateway) will be initiated. The firewall will authenticate the group authentication name and password. If the group authentication settings are valid, the IPSec connection is established.
4. The Live Scan or Card Scan device will then Email the NIST submission DIRECTLY to the NIGC Fingerprint Internet Mail server using (SMTP) and it should be addressed to an address provided by the NIGC (normally triberelay@NIGCEXT01.NIGC.GOV). In turn, the NIGC Fingerprint Internet Mail server will be forwarded to the NIGC's SnF server. We do not allow split tunneling or routing the submission to an outside server before being sent to NIGC Fingerprint Internet Mail server.
5. The SnF server will parse the submission, retaining all information in the SnF database and perform various data analysis (edit checks) to ensure a proper submission. During the edit checks, the SnF will match the OCA field (2.009) to the sender's address to ensure proper accounting and billing. If the SnF server finds an error that prevents processing the submission, the SnF will return an electronic response, similar to the FBI's ERRT (see step 11) and the submission will not be sent to the FBI. After correcting the problem, the tribe should create a new submission (new TCN) and transmit. The tribe will not be charged for the submissions that the SnF rejects.
6. After the submission is processed, the NIGC's SnF server will send the submission to the FBI's IAFIS for processing.
7. The FBI's IAFIS takes anywhere from 20 minutes to 24 hours to process the submission and send a response. The average is 2-3 hours. Once they have completed processing, the FBI will send a response containing either a "no record found" called a Nonident or an Ident. The FBI Rap sheet will be attached if the "Request for Rap Sheet" field (2.070) is set to "Y" for Yes. If this field is missing or set to 'N' for No, the submitter will only receive the Ident record. If you do not receive a response from the NIGC after 24 hours, please contact the NIGC Fingerprint Administrator.
8. The NIGC's SnF server will parse the response, retain all the necessary information in the SnF database and return the response to the tribe's mailbox on NIGC Fingerprint Internet Mail server. The SnF uses the 'From' address of the corresponding submission.

9. The NIGC Fingerprint Internet Mail server will queue the response in the previously associated POP3 account and hold the response until retrieved by the tribe's scan device.
10. The tribe's system will initiate a second IPSec tunnel or L2TP tunnel and connect to their POP3 account to retrieve the queued responses. Submitting systems should be configured to connect no more frequently than once every fifteen minutes to retrieve responses.
11. If the submission has an error or the image quality of the fingerprint images is corrupted or unreadable, the FBI will return a Ten Print Error Transaction (ERRT). This error response lists the problems that occurred in the invalid fields or will describe the image quality problems. This ERRT will be processed and emailed to the submitting tribe and NIGC regional office (See next step).
12. The ERRT will contain the FBI TCN (Transaction Control Reference). This number is quickly identified because it begins with FBI TCN: E200 and is 20 characters long. When the tribe fixes the problem that caused the error, a new submission must be submitted (new TCN (TCR)) and the FBI TCN (Transaction Control Reference) is entered in the TCR (1.10) tag field. This allows the tribe to resubmit the transaction without being billed again.

2.8 Basic Hard Card Fingerprinting Tips

There is no certification requirement with the NIGC to be able to take fingerprints. The only requirement is developing a proficient technique for taking clear, clean fingerprints. The tips here should help you get started, and then all you need is practice.

Basic Fingerprinting Tips

Fill out the top of the fingerprint card first.

All the applicant's information should be on the card and the applicant should sign the card prior to taking the prints. This will avoid accidentally smudging the prints.

Have the applicant wash their hands.

Dirt or other particles on the fingers can obscure characteristics, cause smearing, and create inaccurate marks in the print. If the applicant has excessive perspiration on the hands, wipe each finger with a cloth before inking and then roll the print immediately. Using rubbing alcohol and letting it dry can also temporarily dry the skin enough to allow printing. (If using a live scan instrument, be sure that the fingerprint plate is clean and free of oils, dust, and residue from previous prints before beginning.)

Use only heavy black ink intended for fingerprinting.

Other types of ink smear or do not provide adequate coverage. "Inkless" fingerprint pads do not provide acceptable prints.

Use the right amount of ink.

Not fully inking the finger prior to rolling can result in "gaps" and missing characteristics in the prints. Too much ink can cause heavy smears or obscure the ridges of the print. Too little ink may result in impressions that are too faint. Fingerprints should be dark gray for best results.

Control the person's hand.

Ask the applicant to relax and let you do the work. Asking them to look away from the card may prevent them from unconsciously "helping", which may cause twisting or slipping while trying to roll the finger.

Use the "awkward to easy" roll method.

The boxes on the fingerprint card marked for individual fingers must be rolled fingerprints. Rolled prints are made by rolling the finger or thumb from nail edge to nail edge. The fingerprint should show the surface of the fingerprint from fingertip to just past the first joint on the finger, and the entire print must fit within the blue lines of the box designated for that finger. Grasp the top of the applicant's hand and extend the finger to be printed. Roll in one continuous motion using only enough pressure to make a clear print with no "gaps" in the ink; too much pressure may smear the print. For best results, roll fingers on the right hand toward the right, and fingers on the left hand toward the left, going from "awkward" (where the hand/wrist is most uncomfortable) to "easy" (where the hand/wrist ends up in a comfortable natural position). This helps prevent the person resisting and making unexpected movements as you roll. Thumbs are rolled in the opposite direction than fingers on that hand. After reaching the end of the "roll", lift the finger straight up to avoid smearing or stray ink on the card.

Position the hand well for the "flat" prints.

The bottom row of blocks on the fingerprint card is for pressed or "flat" (also known as "plain") impressions. Make sure all four fingers are extended straight and stiff from the hand. Position the hand at an approximately 45 degree angle to the card to ensure that all four fingers will fit into the box. Print as much of the fingers as you can fit, but at least to just past the first joint. Print all four fingers at the same time by pressing down; no "rolling".

Press down slightly on the top of the applicant's fingers to ensure a complete print with no "gaps" and then lift straight up. Thumbs are pressed straight down into the designated block next to the finger impressions. Use care not to overlap the prints or the lines of the boxes.

Use careful technique for "worn" fingerprints.

Some applicants may have "worn" fingerprints with thin or faint ridges. Use less ink, not more, and light pressure to achieve the best results. Squeezing the finger or "milking" it by rubbing down along the length of the finger toward the tip may help raise the ridges.

If you are going to fingerprint on-site at your tribe, then you will need to obtain black fingerprinting ink. Inkless, gel, and watermark ink do not yield acceptable fingerprints. The NIGC does not provide fingerprinting ink.

2.9 Protection of the Fingerprint Card Prior to Submission

TGRAs must have quality assurance processes for protecting the integrity of the fingerprint card and preventing tampering with the card from the time the prints are taken through the submission process.

Suggestions and recommendations for tampering prevention processes can be found in the National Crime Prevention and Privacy Compact Council's *Identity Verification Program Guide* located at <https://www.fbi.gov/services/cjis/compact-council>. Recommendations include:

- Implement forms to standardize the information gathered with each applicant and document the type of photo identification presented by the applicant.
- Establish procedures that use specially sealed envelopes, tribe specific stamps, etc. for the tribe to use as part of a chain-of-custody process for manually captured fingerprints.

2.10 Required Information for Each Fingerprint Card Submission

The following information is intended to assist tribal personnel in ensuring that the blocks on the fingerprint card are properly completed. Either tribal personnel or the applicant can fill out the card, but it is the tribe's responsibility to review the information on the card for accuracy and completion, and verify the applicant's identity. If the tribe fills out the card, the applicant should review the card for accuracy before signing it. Errors, missing information, and information placed in the wrong areas can all cause delays in processing. Please type or print legibly in black ink.

2.10.1 Fingerprint Card Legend

1. **Applicant's full name:** The name should be in the last name, first name, middle name sequence.
2. **Signature:** This is the applicant's signature. Please ensure that the applicant has signed the card in INK.
3. **Residence Address:** This is the applicant's physical residential address, NOT the mailing address.
4. **Aliases (AKA):** Enter any known aliases, including maiden names.
5. **ORI:** Only fingerprint cards indicating the National Indian Gaming Commission (USNIGC00Z) may be used. The block should be preprinted with "USNIGC00Z – Natl Ind Gaming Comm, Washington, DC".
6. **Date of birth (DOB):** The date of birth should be in MM/DD/YYYY format.
7. **Date:** This is the date the applicant was fingerprinted.
8. **Signature of Official Taking Prints:** The signature of the person at the tribe or office taking the prints should be placed in this box.
9. **Your No. OCA:** The submitting tribe's OCA should be written here. This alphanumeric identifier is nine characters long.

10. **Sex:** **M** for Male, **F** for Female

11. **Race:** Enter the one letter abbreviation for race.

A Asian/Pacific Islander

B Black

I American Indian or
Alaskan Native

W White or Hispanic

U Unknown

12. **Height:** Enter the height in feet and inches. Example: An applicant who is 5 feet 7 inches tall should be entered as 507, not 67 inches. An applicant who is 5 feet 10 inches tall should be entered as 510.

13. **Weight:** Enter the weight in pounds as a whole number. Numbers under 100 should be entered as three numbers with a leading zero. Example: 95 pounds should be entered as 095.

14. **Eye & Hair Color:** Enter the three letter abbreviation for the applicant's eye and hair color.

EYE COLOR

BLK Black

BLU Blue

BRO Brown

GRN Green

GRY Gray

HAZ Hazel

MAR Maroon

MUL Multicolored

PNK Pink

HAIR COLOR

BLK Black

BLN Blond or Strawberry

BLU Blue

BRO Brown

GRN Green

GRY Gray or Partially Gray

ONG Orange

PLE Purple

PNK Pink

RED Red or Auburn

SDY Sandy



WHI White

XXX Unknown or Completely
Bald

15. **Place of birth:** If born in the United States, enter the two letter state abbreviation (e.g., AZ). If the place of birth is a foreign country, enter the full name of the country (do not abbreviate).

16. **Employer and Address:** Enter the name and address of the tribe that is submitting the fingerprint card. This tribe must be the same tribe that is assigned to the OCA written in the “Your No. OCA” block.
17. **Reason fingerprinted:** Enter “Indian Gaming Licensee”.
18. **Social Security Number:** Enter the social security number of the applicant in XXX - XX - XXXX format. If the applicant does not have a social security number, leave this blank.
19. **Rolled prints in proper box for each finger:**
- A complete set of inked fingerprint impressions must be submitted.
 - Fingerprints must be rolled from side of nail to side of nail. All impressions must be within the correct blue box for that print with no overlapping.
 - All impressions should be taken in proper order. The prints must be legible and classifiable.
 - If a finger cannot be printed, indicate a reason in the correct finger block:
 - For a finger that was physically severed and is missing the first joint or more, you may enter "AMP" in the correct box for that finger. If the finger has been physically missing the first joint or more since birth, it is also acceptable to write "missing since birth".
 - If a portion of the first joint is still present ("tip amputated"), print the available fingerprint remainder as you normally would. If a finger is present but severely scarred, print it as you normally would.
 - Attempt to fingerprint deformed fingers; use a notation only if attempts to print have failed. If the finger cannot be printed due to injury (such as a broken bandaged finger) or severe deformation, indicate the reason for the missing print in the correct fingerprint box (e.g., "bandaged", "injured", "paralyzed").
 - See the reverse side of the card for information regarding requirements in taking a good set of fingerprints. The FBI website at www.fbi.gov offers tips for taking proper legible fingerprints. Type *Recording Legible Fingerprints* and *Capturing Legible Fingerprints* in the website search box to find these tips.
 - If a rolled print is smeared or otherwise unacceptable, you may cover it with an adhesive tab and try again. No more than two retabs may be used on a single fingerprint block.
20. **Pressed simultaneous prints in proper boxes:** Do not roll fingerprints in these boxes: these are known as "flat" or "slap" prints. Fingers are pressed down together and then lifted straight up. Thumbs are pressed down separately in the appropriate box. Ensure prints are placed in the proper boxes with no overlapping. Do not overlap the blue lines of the box.

2.11 Example Fingerprint Card

APPLICANT		LEAVE BLANK		TYPE OR PRINT ALL INFORMATION IN BLACK				FBI		LEAVE BLANK	
SIGNATURE OF PERSON FINGERPRINTED		SIGNATURE OF APPLICANT		ALIASES <u>AKA</u>		OR I		USNIGC00Z		DATE OF BIRTH <u>DOB</u>	
RESIDENCE OF PERSON FINGERPRINTED		STREET ADDRESS		OTHER NAMES		INCLUDING MAIDEN		MM/DD/YYYY		PLACE OF BIRTH <u>POB</u>	
CITY, STATE, ZIP		DATE		FINGERPRINT TECH NAME/ID #		CITIZENSHIP <u>CTZ</u>		SEX	RACE	HGT	WGT
DATE OF OFFICIAL TAKING FINGERPRINTS		YOUR NO. <u>OCA</u>		YOUR TRIBE'S OCA		ARMED FORCES NO. <u>MNU</u>		SEX	RACE	HGT	WGT
EMPLOYER AND ADDRESS		NAME OF TRIBE		MAILING ADDRESS		SOCIAL SECURITY NO. <u>SOC</u>		EYES	HAIR	HAIR	STATE
CITY, STATE ZIP		INDIAN GAMING LICENSEE		SOCIAL SECURITY #		LEAVE BLANK					
CLASS		REF.									
→ ROLL PRINTS		Right thumb		Right index finger				Right ring finger		Right little finger	
1. R. THUMB		2. R. INDEX		3. R. MIDDLE		4. R. RING		5. R. LITTLE			
→ ROLL PRINTS		Left thumb		Left index finger		Left middle finger		Left ring finger		Left little finger	
6. L. THUMB		7. L. INDEX		8. L. MIDDLE		9. L. RING		10. L. LITTLE			
→ PRESS PRINTS FLAT		Left four fingers taken at the same time		Left thumb		Right thumb					
LEFT FOUR FINGERS TAKEN SIMULTANEOUSLY		L. THUMB		R. THUMB		RIGHT FOUR FINGERS TAKEN SIMULTANEOUSLY					

2.12 Payment and Submission Packets

This subsection contains fee information and payment submittal requirements.

2.12.1 Fees

(Current fees as of November 1, 2019)

Current fee per fingerprint submission	\$22.00 per card
Resubmission due to rejection if using the Transaction Control Numbers	\$0 per card
Search requests if using the Transaction Control Numbers	\$0 per card request

2.12.2 Payment Submittal Requirements

Fingerprint statements are processed on a monthly basis and mailed to the tribe address and contact provided to the NIGC. Payments of fingerprint fees are due within 30 days of the fingerprint statement.

The NIGC DOES NOT accept personal checks, cash, or credit/debit cards.

Make the payment instrument payable to the **National Indian Gaming Commission**.

2.13 Rejected Fingerprint Cards/Resubmissions

When fingerprint submissions are rejected, you will receive a NIGC and/or an FBI notice with the reason for the rejection.

If cards are rejected for incomplete/inaccurate information, carefully follow the instructions on the reject notice.

If the fingerprint cards were rejected because the fingerprints are illegible or unclassifiable, a new fingerprint card will be needed. Always include a copy of the reject notice/FBI reject sheet with your resubmission

Example FBI Reject Sheet

REJECT
1.01: 158
1.02: 0201
1.03: 1
1.04: ERRT
1.05: 20021124
1.06: 4
1.07: WVIAFIS0Z
1.08: WVIAFIS0Z
1.09:
IFCS000X151902662170
1.10: 2A09000030
1.11: 00.00
1.12: 00.00
2.001: 466
2.060: L0008 - THE QUALITY OF THE CHARACTERISTICS IS TOO LOW TO BE USED. HOWEVER, POSSIBLE CANDIDATES WERE FOUND. PLEASE SUBMIT A NEW SET OF FINGERPRINTS FOR COMPARISON TO THE CANDIDATE(S).
Reason for reject ▲

Applicant cards rejected by the FBI for poor print quality can be resubmitted ONCE free of charge; however, the resubmitted card MUST be received by the FBI within one calendar year of the date of the original reject.

2.13.1 Routine Name Search Procedure

A routine name search procedure requests the FBI to use the name, date of birth, and Social Security number of the applicant whose fingerprints have been rejected twice by the FBI to make a physical search and comparison of their fingerprints to any fingerprint records on file matching their personal information. A fingerprint expert will conduct an examination of the fingerprints and determine with a degree of certainty, if possible, that the prints the tribe submitted did or did not match the records on file at FBI. If they do match, the records on file will be reported to the NIGC and shared with the tribe.

The tribe must follow the routine name search procedure if the fingerprints are rejected twice because the fingerprints are illegible or unclassifiable by the automated process or if the tribe is required to present a page with the applicant's name on it to prove negative FBI name search results.

Routine Name Search Procedure

- 1) The fingerprints must have been rejected twice by the FBI.
 - a) The first reject must be within the past year.
 - b) The name search request must be submitted within 90 days following the second reject.

- 2) The tribe must complete and submit the CJIS Name Search Request Form located in Appendix D of this guide. The TCN is the number below the bar code on the fingerprint card. Enter the TCN of the last two fingerprint cards that were rejected by the FBI. Write your tribe's OCA in the OCA field. When the form is completed, FAX the form to the NIGC Systems Specialist. It takes two to three weeks to receive the results back from the FBI depending on their volume. The results will be forwarded to your Tribe.

If the FBI cannot process the request they will fax it back with a reject notice indicating why they could not complete the request.

A copy of the CJIS Name Search Request can be found in Appendix E.

2.13.2 Example Individual FBI Reject Notice

	REJECT
	1.01: 158
	1.02: 0201
	1.03: 1
(1)	1.04: ERRT
	1.05: 20021124
	1.06: 4
	1.07: WVIAFIS0Z
	1.08: WVIAFIS0Z
(2)	1.09: IFCS000X151902662170
(3)	1.10: 2A09123457
	1.11: 00.00
	1.12: 00.00
	2.001: 466
	2.002: 00
(4)	2.006: XX000000E
	2.007:
(5)	2.060: L0008 - THE QUALITY OF THE CHARACTERISTICS IS TOO LOW TO BE USED.
(6)	2.073: USNIGC00Z
	2.092:
	2.128:
	2.600:

FBI Reject Notice Legend

- (1) Error message

- (2) Information used by NIGC for resubmission
- (3) TCN assigned by NIGC
- (4) Submitting Tribe's OCA
- (5) Reject code and reason for reject
- (6) NIGC ORI

2.14 Example FBI Criminal History Record

Federal Criminal History Record Legend

- (1) Information used by NIGC for resubmission
- (2) PCN assigned by NIGC
- (3) Submitting Tribe's OCA
- (4) Subject's name
- (5) IDENT (indicates an FBI record)
- (6) NIGC's ORI
- (7) Subject's name
- (8) Subject's personal identifiers
- (9) Federal use and dissemination restrictions
- (10) Warrant notification
- (11) Warrant
- (12) Arrest information
- (13) Offenses/Charges
- (14) Information regarding disposition
- (15) Arrest information
 - Date of arrest or date fingerprint card received by FBI
- (16) Court information
 - Sentence (look for the disposition here for above arrest)
- (17) Arrest information (second arrest – different date and agency)
 - No court and no disposition noted in example
- (18) CRIMINAL HISTORY – Introduces criminal history record information from a state's criminal justice information system.
- (19) CYCLE – Some states use cycle numbers to separate arrest from one another.
- (20) ARRESTING AGENCY - Contains the arresting agency's name and ORI. The first two characters of the ORI are the state abbreviation.

(21) Some states also provide prosecution agency information.

NOTE:

The FBI criminal history record consists of different formats from each state's criminal justice information system. When reading the FBI criminal history record, look for key terms such as arrest, charge, count, court, disposition, level, sentence, severity, etc.

- 1.01:178
- 1.02:0500
- 1.03:11-200
- 1.04:SRE
- 1.05:20161118
- 1.06:4
- 1.07:USNIGC00Z
- 1.08:WVIAFIS0Z
- (1) 1.09:E20160000000000000000
- (2) 1.10:2A09123456
- 1.11:00.00
- 1.12:00.00
- 1.13:00.00

- 2.001:0000
- 2.002:00
- (3) 2.006:XX000000E
- 2.014:000000000
- (4) 2.018:SMITH, BRAD
- (5) 2.059:I
- (6) 2.073:USNIGC00Z

UNITED STATES DEPARTMENT OF JUSTICE
 FEDERAL BUREAU OF INVESTIGATION
 CRIMINAL JUSTICE INFORMATION SERVICES DIVISION
 CLARKSBURG, WV 26306

USNIGC007Z
 PCN 2A09123456

THE FBI IDENTIFIED YOUR TEN-PRINT SUBMISSION WHICH
 CONTAINED THE FOLLOWING DESCRIPTORS:

- (7) NAME SMITH, BRAD

- (8)

SEX	RACE	BIRTH DATE	HEIGHT	WEIGHT	EYES	HAIR
M	W	1954/01/11	603	235	BROWN	BLACK

STATE ID	BIRTH PLACE
NULL	TEXAS

OTHER BIRTH DATES	SOCIAL SCARS-MARKS-TATTOOS	SECURITY	MISC NUMBERS
NONE	NONE	000-00-0000	NONE

 ALIAS NAME(S)
 NONE

 END OF COVER SHEET

UNITED STATES DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES DIVISION
CLARKSBURG, WV 26306

USNIGC007Z
NCNE20160000000000000000

BECAUSE ADDITIONS OR DELETIONS MAY BE MADE AT ANY TIME, A NEW COPY SHOULD BE REQUESTED WHEN NEEDED FOR SUBSEQUENT USE.

THIS RECORD IS SUBJECT TO THE
FOLLOWING USE AND DISSEMINATION RESTRICTIONS

- (9) UNDER PROVISIONS SET FORTH IN TITLE 28, CODE OF FEDERAL REGULATIONS (CFR) SECTION 50.12, BOTH GOVERNMENTAL AND NONGOVERNMENTAL ENTITIES AUTHORIZED TO SUBMIT FINGERPRINTS AND RECEIVE FBI IDENTIFICATION RECORDS MUST NOTIFY THE INDIVIDUALS FINGERPRINTED THAT THE FINGERPRINTS WILL BE USED TO CHECK THE CRIMINAL HISTORY RECORDS OF THE FBI. IDENTIFICATION RECORDS OBTAINED FROM THE FBI MAY BE USED SOLELY FOR THE PURPOSE REQUESTED AND MAY NOT BE DISSEMINATED OUTSIDE THE RECEIVING DEPARTMENT, RELATED AGENCY OR OTHER AUTHORIZED ENTITY. IF THE INFORMATION ON THE RECORD IS USED TO DISQUALIFY AN APPLICANT, THE OFFICIAL MAKING DETERMINATION OF SUITABILITY FOR LICENSING OR EMPLOYMENT SHALL PROVIDE THE APPLICANT THE OPPORTUNITY TO COMPLETE, OR CHALLENGE THE ACCURACY OF, THE INFORMATION CONTAINED IN THE FBI IDENTIFICATION RECORD. THE DECIDING OFFICIAL SHOULD NOT DENY THE LICENSE OR EMPLOYMENT BASED ON THE INFORMATION IN THE RECORD UNTIL THE APPLICANT HAS BEEN AFFORDED A REASONABLE TIME TO CORRECT OR COMPLETE THE INFORMATION, OR HAS DECLINED TO DO SO. AN INDIVIDUAL SHOULD BE PRESUMED NOT GUILTY OF ANY CHARGE/ARREST FOR WHICH THERE IS NO FINAL DISPOSITION STATED ON THE RECORD OR OTHERWISE DETERMINED. IF THE APPLICANT WISHED TO CORRECT THE RECORD AS IT APPEARS IN THE FBI'S CJIS DIVISION RECORDS SYSTEM, THE APPLICANT SHOULD BE ADVISED THAT THE PROCEDURES TO CHANGE, CORRECT OR UPDATE THE RECORD ARE SET FORTH IN TITLE 28, CFR, SECTION 16.34.

FBI IDENTIFICATION RECORD -

WHEN EXPLANATION OF A CHARGE OR DISPOSITION IS NEEDED, COMMUNICATE DIRECTLY WITH THE AGENCY THAT FURNISHED THE DATA TO THE FBI.

- (10) *****NOTICE*****
SUBJECT OF RECORD IS WANTED
SEE END OF RECORD FOR MORE INFORMATION

END OF PART 1 - PART 2 TO FOLLOW

UNITED STATES DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES DIVISION
CLARKSBURG, WV 26306

USNIGC007Z
PART 2

NCNE20160000000000000000

FBI IDENTIFICATION RECORD - FBI UCN-000000000

NAME SMITH, BRAD FBI UCN 00000000 DATE REQUESTED 2016/11/18

SEX RACE BIRTH DATE HEIGHT WEIGHT EYES HAIR
M W 1954/01/11 603 235 BROBLK

BIRTH PLACE
TEXAS

PATTERN CLASS CITIZENSHIP
UNITED STATES
AU WU RS WU WU AU LS LS WU
LS RS
RS

(11)

* WANTED *
* *
* CONFIRM THAT WARRANT IS STILL OUTSTANDING *
* *
* AGENCY-SHERIFF'S OFFICE CROWN POINT (IN0450000)
*
* WANTED-NCIC#W000000000 *
* DAVIS, BRAD *
* FAILURE TO APPEAR - SEE MIS (IDENTIFY *
* ORIGINAL OFFENSE) *
* CASE #0000000 *
* DATE OF WARRANT 01/07/2014 *
* NOTIFY IN0450000 SHERIFF'S OFFICE CROWN POINT IN *

RECORD UPDATED 2016/11/18

OFFENDER NAME	STATE ID	FBI NUMBER	NUMBER
SMITH, BRAD		IN0000000	000000000
SEX RACE BIRTH DATE HGT WGT EYES HAIR PLC OF BIRTH			
M	W	1954/01/11	603 235 BRO BLK TX
FINGERPRINT CLASS			

NCIC:

HENRY UP:

HENRY LOW:

NO ALIAS INFORMATION IS ON FILE FOR THIS SID.

NO SCARS, MARKS, OR TATTOOS IS ON FILE FOR THIS SID.

SOCIAL SECURITY

000000000

ARREST -01 20130101

(12) AGENCY: HOBART POLICE DEPT (IN0450900)

AGENCY CASE: 000000

(13) ARREST CHARGES:

CHARGE 01:001 OF DWS - PRIOR 1 COUNTS

CHARGE 02:001 OF FAILURE TO APPEAR 1 COUNTS

CHARGE 03:001 OF HOLD FOR MERRILLVILLE1 COUNTS

(14) NO DISPOSITION INFORMATION IS ON FILE FOR THIS ARREST

NO CUSTODY INFORMATION IS ON FILE FOR THIS SID

THE DATA LISTED ON THE TRANSCRIPT MAY NOT BE AN EXACT REPLICATION OF THE DATA SUPPLIED BY THE ARRESTING AGENCY. TO RECEIVE THE EXACT CHARGE INFORMATION, A CERTIFIED TRANSCRIPT MUST BE REQUESTED.

END OF KNOWN RECORD

END OF RECORD

END OF RECORD

=====

2.2008:SMITH, BRAD

2.2031:11

UNITED STATES DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES DIVISION
CLARKSBURG, WV 26306

USNIGC007Z
PART 2

- FBI IDENTIFICATION RECORD - FBI NO. 123456AZ7

- (15) 1 - ARRESTED OR RECEIVED 1989/07/11
AGENCY-SHERIFF'S OFFICE RIVERSIDE (CA0330000)
AGENCY CASE-20987
CHARGE 1-POSS NARC C/S
- (16) COURT-COUNTY COURT RIVERSIDE
CHARGE-11350 HS-POSSESS NARCOTIC CONTROL SUBSTANCE
SENTENCE-
DIVERSION DISMISSED
- (17) 2 - ARRESTED OR RECEIVED 1995/02/13
AGENCY-POLICE DEPARTMENT FRESNO (CA0100500)
AGENCY CASE-8502137001
CHARGE 1-DRIVING WITH LICENSE INVALID
- 3 - ARRESTED OR RECEIVED 2005/05/26
AGENCY-POLICE DEPARTMENT CEDAR PARK (TX2460900)
AGENCY CASE-56302
CHARGE-AGG ASSAULT SBI
- COURT-26TH DISTRICT COURT GEORGETOWN (TX246015J)
CHARGE-AGG ASSAULT CAUSES SERIOUS BODILY INJURY
SENTENCE-
2006-04-23 DEFERRED PRB-5Y0MOD FNE-2500
- 4 - ARRESTED OR RECEIVED 2011/09/03
AGENCY-SHERIFF'S OFFICE GEORGETOWN (TX2460000)
AGENCY CASE-11586
CHARGE-THEFT>\$20<\$500 BY CHECK
- COURT-COUNTY COURT GEORGETOWN (TX246013J)
CHARGE-THEFT CLASS C MISDEMEANOR
SENTENCE-
2011-12-01 CONVICTED LESSER CHARGE FNE-0200

ALL ARREST ENTRIES CONTAINED IN THIS FBI RECORD ARE BASED ON
FINGERPRINT COMPARISONS AND PERTAIN TO THE SAME INDIVIDUAL

THE USE OF THIS RECORD IS REGULATED BY LAW. IT IS PROVIDED FOR OFFICIAL
USE ONLY AND MAY BE USED ONLY FOR THE PURPOSE REQUESTED.

(18)

```
*****CRIMINAL HISTORY*****
===== CYCLE 1 =====
Tracking Number      1463714637
Earliest Event Date  1997-03-01
-----
Arrest Date          1997-03-01
Arresting Agency     CO0340100 DURANGO POLICE DEPARTMENT
Subject's Name
Comment(s)           MNU#: OA-970000
Charge               1
Charge Literal       ASSAULT
Statute              ASSAULT 3RD DEG (1399)
Counts               1
Severity             MISDEMEANOR
```

(19)

```
*****CRIMINAL HISTORY*****
===== CYCLE 001 =====
TRACKING NUMBER      00066384102
EARLIEST EVENT DATE  2001-03-21 INCIDENT DATE      2001-03-21
-----
```

(20)

```
ARREST CASE NUMBER   10301 6E
ARRESTING AGENCY     GA0460100 VIENNA POLICE DEPARTMENT
SUBJECT'S NAME
ARREST TYPE          ADULT
CHARGE               1
CHARGE NUMBER        00066384102001
CHARGE TRACKING NUMBER 0066384102
CHARGE LITERAL       DISORDERLY CONDUCT
STATUTE              DISORDERLY CONDUCT {16-11-39; GA}
STATE OFFENSE CODE   5311
SEVERITY             MISDEMEANOR
-----
```

```
COURT DISPOSITION    {CYCLE 001}
COURT AGENCY         GA046031J VIENNA RECORDERS COURT
SUBJECT'S NAME
CHARGE               1
CHARGE NUMBER        00066384102001
CHARGE TRACKING NUMBER 00066384102
CHARGE LITERAL       DISORDERLY CONDUCT
STATUTE              DISORDERLY CONDUCT {16-11-39; GA}
STATE OFFENSE CODE   5311
SEVERITY             MISDEMEANOR
DISPOSITION          {CONVICTED 2001-04-18; BOND FORFEITURE}
```

<CRIMINAL HISTORY INFORMATION>

```
LAST ARRESTED:      01/19/1997
ARREST AGENCY:      HONOLULU PD
TOTAL ARRESTS:      2
TOTAL CHARGES:      2
ARREST: 1 OF 2
ARREST DATE/AGENCY: 01/19/1997 HONOLULU PD
OBTS TRACKING NUMBER: 30261H4
CRIME TYPE:
CHARGE: 1 OF 1
CHARGE              STATUTE          SV          FC
ARREST/FILING:     ASSAULT 2          707-0711    SV          FC
FINAL/LAST:         ASSAULT 2          707-0711    SV          FC
ARREST REPORT:     97-025036
(SV = SEVERITY FC=FELONY CLASS C)
FINAL/LAST: AGENCY: HONOLULU FAM CT
CASE NO: FC97-0001
DISP/DATE: GUILTY          05/06/1997
DAGRETURN:
SENTENCE:           ON 05/06/1997, SUBJECT WAS SENTENCED TO 50 HOUR(S)
COMMUNITY SERVICE, 5 YEAR(S) PROBATION, AND $372
RESTITUTION.
```

***** CRIMINAL HISTORY *****

===== CYCLE 001 =====

Tracking Number 00000000100
Earliest Event Date 2004-12-03 Incident Date 2005-01-11

Arrest Date 2005-01-11
Arresting Agency KS0260000 ELLIS COUNTY SHERIFF'S OFFICE HAYS

Subject's Name
Arrest Type Adult
Comments Fingerprinted on 2005-01-11.

Charge 1
Charge Literal Worthless check; Unknown value
Charge Description Non-Person Offense
Statute Giving a worthless check; Unknown value
(21-3707 KS)
Counts 1
Severity Unknown
Disposition Other(Referred to prosecutor.)

Booking Case Number 05-025

Prosecutor Disposition (Cycle 001)
Prosecutor Case Number 04CR000
Prosecution Date 2004-12-03
Prosecutor Agency KS026013A ELLIS COUNTY ATTORNEY'S OFFICE HAYS
Subject's Name

Charge 1
Charge Literal Worthless check; Misd
Charge Description Non-Person Offense
Statute giving worthless check; Misdemeanor (21-3707 KS)
Counts 1
Severity Misdemeanor Class A

Disposition Diversion(Diversion completed)
Prosecution Comment Diversion initiated on 2005-01-11. Diversion
Period 6 months. Diversion completed on
2005-07-11.
Prosecution Comment Dismissed with prejudice 07/11/05

*****CRIMINAL HISTORY*****

===== CYCLE 001 =====

Tracking Number 001
Earliest Event Date 2002-12-15

Arrest Date 2002-12-15
Arrest Case Number 2702027020

Arresting Agency FL0069000
FLORIDA HIGHWAY PATROL - FT.

LAUDERDALE
Arrest Type ADULT
Charge 001
Charge Number 2702027020
Charge Tracking Number 060701060701
Charge Literal DUI-UNLAW BLD ALCH-
Agency FL0069000
FLORIDA HIGHWAY PATROL - FT.

LAUDERDALE
Charge Description DUI ALCOHOL OR DRUGS 1ST OFFENSE
Statute DUI ALCOHOL OR DRUGS (FL316.193(2A);FL

(21)

)

NCIC Offense Code 5407
Counts 001
Severity MISDEMEANOR
Enhancing Factor 2ND DEGREE

Prosecutor Disposition (Cycle 001)
Prosecution Date 2002-12-15
Prosecutor Agency FL006023J BROWARD COUNTY COURT
Charge 001
Charge Number 001
Charge Tracking Number 060701060701
Charge Literal DUI-UNLAW BLD ALCH-
Charge Description Suppl Arr Degree:1ST
Charge Description Suppl Arr Level:MISDEMEANOR
Charge Description DRIVING UNDER THE INFLUENCE
Charge Description COUNSEL TYPE:OTHER
Statute DUI ALCOHOL OR DRUGS (FL316.193(1);)
NCIC Offense Code 5407
Counts 001
Severity MISDEMEANOR
Enhancing Factor 1ST DEGREE
Disposition (Other 2003-01-15; FILED
)

Court Disposition (Cycle 001)
Court Disposition Date 2003-01-21
Court Case Number 0000000000001MI
Court Agency FL006023J
BROWARD COUNTY COURT
Charge 001
Charge Number 001
Charge Tracking Number 060701060701
Charge Literal DUI-UNLAW BLD ALCH-
Charge Description DRIVING UNDER THE INFLUENCE
Charge Description COUNSEL TYPE:OTHER
Charge Description TRIAL TYPE:NONE
Charge Description PLEA TYPE:NOLO CONTENDRE
Statute DUI ALCOHOL OR DRUGS (
FL316.193(1)
;)

NCIC Offense Code 5407
Counts 001
Severity MISDEMEANOR
Enhancing Factor 1 ST DEGREE
Disposition (Convicted 2003-01-21; GUILTY/CONVICTED
)

Sentencing (Cycle 001)
Sentence Date 2003-01-21
Sentencing Agency FL006023J BROWARD COUNTY COURT
Court Case Number 0000000000001MI
Charge 001
Charge Number 001
Charge Literal DUI-UNLAW BLD ALCH-
Sentence
PROBATION-06M
Sentence
FINE- \$263.00
Sentence
COURT COST- \$26.00
Sentence
COURT PROVISION - COMMUNITY SERVICE
Sentence

COURT PROVISION - ATTEND DWI SCHOOL

Sentence

COURT PROVISION - ABIDE BY COURT RESTRICTIONS

===== CYCLE 002 =====

Tracking Number 002

Earliest Event Date 2012-08-29 Incident Date 2012-08-29

Arrest Date 2012-08-29

Section 3 - Basic Privacy & Security Guidelines

Access, use, handling, dissemination, and destruction of criminal justice information (CJI) and criminal history record information (CHRI) is governed by federal and state laws, rules, regulations and policies. The receiving organization is responsible for maintaining the confidentiality and control of any CJI/CHRI it obtains.

CJI/CHRI may only be used for the specific purpose for which it was requested (employment, licensing, volunteers, etc.). For more information regarding the FBI CJIS Security Policy please visit <https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center>. The policy is updated periodically so the Tribe must check the website often to ensure the correct FBI CJIS Security Policy is being used. Sample policies for Proper CHRI Access, Use, Handling and Dissemination can be found in Appendix F.

3.1 Policies and Procedures

The Tribe must establish policies/procedures in the following CJI/CHRI privacy and security areas, and ensure all organization personnel are aware of them.

- Access:
 - Defining who is authorized to access CJI/CHRI (Authorized Personnel)
 - Restricting access to only those who are authorized
- Use:
 - Defining the authority, purpose and use of the CJI/CHRI. In the case of CJI/CHRI obtained through NIGC via IGRA, the purpose and use is for licensing and/or employment of key employees and primary management officials of tribal gaming enterprises, as defined by NIGC regulations.
 - Restricting use to the specific purpose for which the CJI/CHRI was requested
- Handling:
 - Proper security of CJI/CHRI from receipt through destruction
 - Retention/destruction rules and processes
- Prevention of unauthorized disclosure of CJI/CHRI:
 - Access-limited storage
 - Not leaving CJI/CHRI unattended when it is not physically secured
 - Revocation of access privileges for terminated employees or those removed from the Authorized Personnel List
 - Processes for ensuring proper training and refresher training of Authorized Personnel
- Communication:
 - Communication among Authorized Personnel
 - Communication with the applicant concerning CJI/CHRI, including the provision of the FBI Privacy Act Statement (dated 2013 or later) and *Noncriminal Justice Applicant's Privacy Rights* notice as well as written notification of the procedures for obtaining a change, correction, or update to their criminal history record as set forth in 28 C.F.R. § 16.34 and the provision of a reasonable amount of time to do so.
- Secondary dissemination procedures (if permitted by law):
 - Tribes may provide an applicant or the applicant's attorney a copy of their criminal history record if the tribe has established a written policy to do so
 - Otherwise, generally, secondary dissemination – or reuse – of CJI/CHRI obtained through the NIGC is not permitted.
 - Logging/tracking procedures
 - Procedures for authenticating recipients of the disseminated information
- Formal disciplinary procedure:
 - Steps to be taken by the organization in the event of misuse of CJI/CHRI
 - Specify applicable misconduct policies

- Digital security (if CJI/CHRI scanned or stored electronically):
 - Technical safeguards to protect the access and integrity of confidential information
 - Monitoring and restricting access to databases containing CJI/CHRI, including employing required identification and authentication measures
 - Reporting, response, and handling capability for information security incidents
 - Employing a formal sanctions process for personnel that fail to comply with information security policies and procedures, including those mandated by the CJIS Security policy
 - Ensuring all Authorized Personnel have taken the requisite security awareness training in accordance with the CJIS Security policy
 - Undertaking information technology security audits in accordance with the CJIS Security policy

Additionally, Agencies must have established processes for fingerprint submissions which include:

- Quality assurance measures for applicant identity verification. (See Section 2.2)
- Quality assurance measures for protecting the integrity of the fingerprint card. (See Section 2.12)
- Processes to ensure compliance with federal laws for FBI fingerprint checks (if applicable). (See Section 2.3)

The Tribe must consider the following basic guidelines when formulating policies, procedures, and training.

3.2 Applicant Process

It is the policy of the NIGC to allow the tribe to discuss and provide the criminal record contents with the applicant within the confines of the purpose for which it was provided (i.e. licensing and/or employment of key employees and primary management officials of tribal gaming enterprises):

- The tribe may tell the applicant that there is a factor in the criminal history check that may be disqualifying and discuss that factor with the applicant in order to ascertain if the circumstances of the issue warrant denial.
- To facilitate the challenge/correction process, NIGC permits tribe to supply the applicant or the applicant's attorney with a copy of their FBI criminal history record for review and possible challenge, correction, or update. This courtesy saves the applicant the time and additional fee required in obtaining the record directly from FBI. (See Section 3.3)

3.3 Applicant Review and Challenge of Criminal History

It is the tribe's responsibility to notify applicants in writing of the opportunity and ability to review and challenge their criminal history record. If an applicant believes that their criminal history record is inaccurate or incomplete, refer the person to one of the options below to begin the review and challenge process.

- For a copy of an FBI criminal history record directly from the tribe:
 - The tribe must have adopted written policies and procedures that allow the subject of an FBI record to request a copy of their own record. The policy must include how the request is made; the amount of time to provide the report; how the report will be provided and, if provided by the tribe, how it will be marked to distinguish it as a copy; verification of the applicant's identity; and when the report was provided. Additionally, the Tribe must provide a reasonable amount of time for the applicant to complete or correct the report before the final licensing or employment determination is made. Ensure the applicant is aware that the CHRI provided to the applicant MAY NOT be reused for employment or licensing purposes by any other entity or agency.
- For a copy of an FBI criminal history record directly from the FBI:

- Federal law and U.S. Department of Justice regulations allow the subject of an FBI record to request a copy of their own record. The individual may submit fingerprints, an Applicant Information Form, and payment directly to the FBI according to the procedures in Title 28 C.F.R. §16.30 - 16.34.
- FBI contact phone for information about record review and challenge: (304) 625-5590.
- Submittal forms, checklists, and more information on how to review and challenge an FBI criminal history record can be found at **www.fbi.gov** under *Criminal Justice Information Services - Identity History Summary Checks*.

If the Tribe received their CHRI from a State, rather than NIGC, and that State specifically prohibits release of CHRI, the applicant **must be referred** to that State for a copy of the State CHRI and to FBI for a copy of the FBI CHRI. Note: Arizona prohibits release of CHRI obtained through their services to applicants.

3.4 Communication/Dissemination

Verbal or written communications regarding CJI/CHRI may only occur between Authorized Personnel and only to carry out the specific purpose for which the information was requested. In the case of CJI/CHRI obtained through the NIGC that purpose is licensing and/or employment of key employees and primary management officials of gaming enterprises, as such are defined in NIGC regulations.

3.4.1 Communication Cautions

Tribal personnel must be aware of the following restrictions and cautions concerning CJI/CHRI:

- CJI/CHRI received from the fingerprint criminal history check process is not public record and may not be released to the public. The tribe may neither confirm nor deny the existence or nonexistence of an individual's criminal history record to the public or to any unauthorized individual or tribe.
- Care must be taken to prevent overhearing, eavesdropping, or interception of communication. Consider using private rooms, closed offices, etc., when discussing CJI/CHRI with other authorized personnel or with applicants.
- Viewing and/or disseminating CJI/CHRI for curiosity reasons is not allowed.
- CJI/CHRI cannot be:
 - Emailed (unless encrypted to CJIS Security Policy standards)
 - Sent electronically via cell phone or other handheld device (including texts or pictures of the hardcopy or computer screen)
 - See FBI CJIS Security Policy at <https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center> for Bring Your Own Device (BYOD) requirements
- CJI/CHRI may be faxed only if:
 - The recipient point is within the tribe or secondary dissemination is authorized. As noted above, secondary dissemination is generally not authorized. (See Section 3.1 & 3.4.2).
 - The recipient has been confirmed by the sender as Authorized Personnel or as an otherwise authorized recipient.
 - The receiving fax is in a secure location controlled by the authorized recipient and the arriving CJI/CHRI is not accessible to unauthorized personnel. The tribe is responsible for the security of all copies of CJI/CHRI.
 - See FBI CJIS Security Policy at <https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center> for encryption requirements
- Personnel must be cautioned regarding common causes of casual unauthorized release of

information: e.g., social networks, discussions with friends/family members, conversations in public places.

- Personnel must be made aware of the threat of social engineering. Social engineering is deliberate manipulation or deception designed to elicit the release of confidential information to unauthorized individuals. If secondary dissemination is permitted, the tribe must develop a method which allows personnel to verify the identity and authorized status of an individual requesting information both inside and outside the tribe.

3.4.2 Secondary Dissemination

The receiving tribe may not provide CJI/CHRI to any other tribe, state, agency or individual unless specifically authorized by law. This is called “secondary dissemination” or “reuse”. To be clear, IGRA does not provide for such secondary dissemination or reuse. And CJI/ CHRI obtained through the NIGC cannot be improperly disseminated beyond tribal personnel directly involved in the key employee and primary management official licensing or employment deliberations.

If permitted by other federal or state law, secondary dissemination can only occur with an authorized recipient. All secondary dissemination must be logged, and the log shall be retained for three years. The log must clearly identify the following:

- a) Date of dissemination
- b) Name of requestor
- c) Name and contact information of requestor’s tribe
- d) Purpose for which information is requested
- e) Specific information being released (i.e., criminal history of name of subject)
- f) The name/identification of the person releasing the information

Do not assume you can disseminate the CHRI, please verify your authorization. There are civil and criminal penalties for unlawful dissemination.

3.5 Physical Security

The Tribe is responsible for the security of the CJI/CHRI from its arrival at the tribe through the point of its complete destruction.

3.5.1 Storage

The results of the FBI record search must be stored in such a manner that only authorized personnel have access and must not be retained longer than needed to fulfill its purpose and satisfy the tribe's regulatory guidelines.

- CJI/CHRI must be maintained at all times in a secure location to prevent access/viewing by unauthorized personnel (i.e., locked file cabinet, locked room, secure perimeter, etc.).
- All visitors (including contractors, maintenance, and outside personnel) to areas where CJI/CHRI is kept must be accompanied by Authorized Personnel at all times. Areas must be locked when unattended. Additionally, check the identification of all visitors, contractors and anyone not on the authorized personnel list who may be entering the restricted, controlled area where CHRI is stored or used.
- Authorized Personnel who are granted access to CJI/CHRI must be aware of their responsibility to protect the confidentiality of the information and take steps accordingly. Examples of this are: turning pages with CJI/CHRI face down on a desk; not leaving information exposed or unattended; turning or covering computer screens to inhibit casual viewing; being aware of

unauthorized individuals who may be “shoulder surfing” or walking by when information is being viewed.

3.5.2 Destruction

When no longer needed for its purpose, CJI/CHRI must be completely destroyed to minimize the risk of unauthorized access and dissemination. Please review NIGC regulations at 25 C.F.R. §556.6(a) and 25 CFR §558.3(e) and the approved tribal gaming ordinance for retention time requirements.

- CJI/CHRI cannot simply be thrown away. The acceptable methods of destruction are shredding or incineration.
- Electronic media holding CJI/CHRI must first be sanitized (overwritten at least three times, degaussed) prior to complete destruction.
- Destruction must be performed or observed by Authorized Personnel who are authorized to access/handle CJI/CHRI or approved outsourced contractors (See Section 1.4).

3.6 Technical/Digital Security

If the CJI/CHRI sheets are stored electronically, or CJI/CHRI derived from the sheets is stored electronically, then the Tribe becomes subject to technical information security requirements.

The requirements for electronic storage and access of CJI/CHRI are contained in the FBI CJIS Security Policy and are in the online FBI CJIS Security Policy Resource Center on the FBI website at <https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center>. Electronic security, encryption, and storage protection requirements in the policy apply to TGRAs converting hardcopy CJI/CHRI into electronic format after receipt; the parts governing direct connect/interface with the state/national electronic criminal justice databases do not apply unless the TGRA has an additional function with direct connect/interface access. TGRAs must have knowledgeable information technology (IT) personnel review the requirements in the Security Policy and ensure that TGRA's system is in compliance.

The following general guidelines also apply to electronic/digital security of CJI/CHRI:

- 1) Criminal Justice Information (CJI/CHRI) must be encrypted:
 - When stored (at rest) outside the boundary of a physically secure location
 - When encryption is used for CJI/CHRI at rest, it must be FIPS 140-2 certified and use a symmetric cipher of at least 128 bit in strength or use the AES symmetric cipher at 256 bit strength.
 - Immediately when transmitted outside the boundary of a physically secure location (two exceptions: 5.13.1.2.2 and 5.10.2 in the FBI CJIS Security Policy)
 - When encryption is used for CJI/CHRI in transit, it must be FIPS 140-2 certified and use a symmetric cipher of at least 128 bit.
- 2) The server must be secure and located on-site either with that Tribe or on a site controlled by the Tribe.
 - The actual location of the computers and servers must have adequate physical security to protect against any unauthorized personnel gaining access to the computer equipment or to any of the stored data.
 - Only Authorized Personnel of the TGRA may have access to the server. IT Personnel who are not Authorized Personnel and have unescorted access to unencrypted CJI/CHRI need FBI Compact Officer approved Outsourcing Agreements. (See Section 1.4)

- See FBI CJIS Security Policy for Cloud storage requirements.
- 3) Authorized Personnel who access CJI/CHRI electronically must complete Level Three of the CJIS Security Awareness Training that pertains to electronic access. Authorized Personnel who maintain electronic CJI/CHRI systems must complete Level Four CJIS Security Awareness Training.
 - 4) The Tribe must manage information system accounts. Requirements include:
 - Processes for activating, reviewing, and disabling accounts.
 - The files where CJI/CHRI is stored must be password-protected.
 - Each individual accessing the CJI/CHRI files must be uniquely identified and have a unique password.
 - Password rules are detailed in the FBI CJIS Security Policy.
 - Processes for authorizing and monitoring remote access (if applicable).
 - Restrictions regarding the use of personally owned electronic devices to access, handle, or store CJI/CHRI.
 - Electronic media protection rules, to include provisions for destruction, which include degaussing, overwriting, or physical destruction of media. (See Section 3.5.2)
 - 5) The computer system must include protective features detailed in the CJIS Security Policy. These include but are not limited to:
 - Partitioning which physically or logically separates user interface services from information storage databases
 - Intrusion detection/malicious code protection
 - Spam and spyware detection/protection
 - 6) A security incident handling policy must be in place that allows users to alert technical personnel to an information security incident such as an unauthorized system intrusion. The incident handling response must include preparation, detection, analysis, containment, eradication, and recovery. Each incident must be tracked and documented, including user response activities.
 - 7) When an incident occurs, a Security Incident Report form must be completed and submitted to the NIGC ISO **within 24 hours** of discovery of the incident. The submitted report must contain a detailed account of the incident, events leading to the incident, and steps taken/to be taken in response to the incident. The NIGC uses the CJIS Security Appendix F.1 form to report these incidents. A copy of the form can be found in Appendix F.

3.7 Consequences for Misuse

The receiving tribe/TGRA has the responsibility to ensure that all personnel are aware of the consequences that may result from unauthorized use of CJI/CHRI.

Federal statutes state that access to CJI/CHRI is subject to cancellation for dissemination outside the authorized recipient(s) (Title 28 U.S.C. §534 and Title 28 C.F.R. §20.33). A Tribe's access to CJI/CHRI via submitted fingerprints may also be suspended or cancelled according to the terms and conditions in the MOU.

Other federal and/or state penalties may apply depending on the circumstances of the release and the specific statute violated. Two examples of United States Code violations are Title 18 U.S.C §641 which deals with theft of public records for personal gain and Title 18 U.S.C §1030 which discusses unauthorized access to protected information via computer.

Unauthorized release could potentially expose the organization and/or individual to civil liability. In addition, an individual may be subject to disciplinary action under his/her employer's misconduct policies.

Section 4 - LASO Responsibilities

As mentioned in Section 1 of this guide, the new Memorandum of Understanding (MOU) will require each tribe to designate a Local Agency Security Officer (LASO). The LASO is the primary liaison between the tribe and the NIGC and is responsible for coordinating tribal compliance with all federal and state laws and regulations pertaining to the access, use, handling, dissemination, and destruction of CJI and CHRI. This section summarizes the primary duties and responsibilities of the LASO. A LASO responsibilities handout can be found in Appendix G.

4.1 Primary Liaison

The LASO functions as the primary liaison with the NIGC for all communication regarding audits, training, and security. The LASO is also the first point of contact for the NIGC in the event of an allegation of criminal history misuse or a security issue involving the criminal history check process. It is important that the LASO's contact information stay updated with the NIGC in order to allow for orderly and timely exchange of information.

The LASO is also expected to serve as the information resource for his/her TGRA. The NIGC will send periodic emails to the LASO to keep agencies updated on changes and events relevant to the noncriminal justice process. The LASO is expected to share this information with the personnel at the TGRA as needed.

The NIGC also maintains a contact person at each TGRA in case of a processing problem. TGRAs may choose to have the LASO serve in both capacities or may choose to have a different person for each, based on the Tribe's organizational structure and need. Both contacts must be kept updated.

4.1.1 Information Changes

In addition to keeping the LASO's contact information updated, the LASO is responsible for keeping the tribe and TGRA's information updated. The LASO must inform the NIGC of changes in the authorized Tribal signatory on the MOU, the LASO, or any relevant business information (Tribe name changes, mailing/physical address changes, etc.). The forms mentioned in this section are in the appendices of this guide and are also available from the NIGC website at <https://www.nigc.gov/compliance/CJIS-Training-Materials>. Forms may be emailed, faxed, or mailed to the NIGC ISO. (See the Contact List on page 5).

If the signatory to the MOU changes:

- The tribe must sign a new MOU within 6 months or access will be suspended.

If the LASO changes:

- The tribe must appoint a new LASO and submit the *Noncriminal Justice Agency Information Change Form* to the NIGC within 30 days of the change. (See Appendix H for a copy of this form or the NIGC website at <https://www.nigc.gov/compliance/CJIS-Training-Materials>.)
- The tribe can also designate a secondary (backup) LASO on this form.
- The NIGC will send an email acknowledgment upon receipt of the notification.

If the authorized Tribal signatory changes:

- Submit the *Noncriminal Justice Agency Information Change Form* to the NIGC. (See Appendix H or the NIGC website at <https://www.nigc.gov/compliance/CJIS-Training-Materials>.) If a new authorized tribal signatory has not been selected, submit the information of the interim/acting authorized signatory and note the anticipated time before permanent replacement in the form's Comments field.

- The NIGC will provide a MOU with instructions for its completion if needed.

If the name, mailing address, physical address, and/or main phone number of the tribe changes:

- Fill out the information you want to change on the *Noncriminal Justice Agency Information Change Form*. (See Appendix H or the NIGC website.)
- The NIGC will acknowledge receipt of the form and update the information. If further information is required, the NIGC will contact the LASO with any questions.

4.1.2 Authorized Personnel List

The LASO must submit an Authorized Personnel List to the NIGC. The Authorized Personnel List contains all TGRA and tribal personnel who are authorized to receive, view, handle, disseminate, store, retrieve, or dispose of CJI/CHRI. The Authorized Personnel List must be submitted by the tribe and must contain the names and titles of the authorized individuals.

Examples of types of personnel a tribe and TGRA may want to authorize:

- Administrative personnel who open the tribe's mail, have filing duties, or perform functions which grant them trusted access to locked/secured areas or access to unsealed CJI/CHRI.
- Personnel involved in licensing eligibility determinations: Gaming Commissioners, Executive Directors, Licensing agents, etc.
- TGRA Information technology personnel (if CJI/CHRI is stored electronically). Please note, IT Personnel who are not Authorized Personnel and have unescorted access to unencrypted CJI/CHRI need FBI Compact Officer approved Outsourcing Agreements. (See Section 1.4)

An example Authorized Personnel List can be found in Appendix I of this guide and also online on the NIGC website at <https://www.nigc.gov/compliance/CJIS-Training-Materials>. The entire Authorized Personnel List must be updated and resubmitted when changes occur (e.g., an individual is no longer authorized to view/handle CJI/CHRI, an authorized individual is no longer employed by the tribe or TGRA, an authorized individual has a name change, personnel turnover, and name/contact information changes). Ensure the LASO is on the Authorized Personnel List. The tribe must retain one copy of the Authorized Personnel List for its records and forward a copy to the NIGC.

4.2 Privacy and Security Coordinator

The LASO is the person primarily responsible for maintaining Tribe compliance with federal and state law and regulations for privacy and security requirements. Compliance duties include:

- Ensuring Authorized Personnel receive required training.
- Updating/maintaining training documentation.
- Updating and submitting Authorized Personnel List to NIGC.
- Ensuring Authorized Personnel have signed the Tribe's Acknowledgement Statement.
- Ensuring the Tribe has adequate policies/procedures related to access, use, handling, dissemination, and destruction of CJI/CHRI.

4.2.1 Required Training for Authorized Personnel

Authorized Personnel must complete two sets of training:

1) CJIS Training:

CJIS Security Awareness Training (SAT) required for all individuals (criminal justice and noncriminal justice) who view or handle CJI and CHRI. All Authorized Personnel must receive CJIS SAT within six months of hire or being placed on the Authorized Personnel List and then every two years thereafter. SAT is designed to explain and clarify points for those individuals who have no background in the criminal justice field. There are four levels of CJIS security awareness training required for each person's access and duties. Level One is for persons with unescorted access to a physically secure location; Level Two is for all authorized personnel with access to CJI; Level Three is for all authorized personnel with both physical and logical access to CJI; and Level Four is for all

Information Technology personnel.

A copy of the FBI CJIS SAT PowerPoint Presentation and a 30 minute NIGC Licensing Update video can be found at the NIGC website at <https://www.nigc.gov/compliance/CJIS-Training-Materials>.

2) Tribe's policies/procedures training:

Each tribe must train Authorized Personnel on the Tribe's internal policies/procedures for the proper access, use, handling, dissemination, and destruction of CJI/CHRI and on the consequences of misuse of CJI/CHRI. This training must be conducted within six months of hire or being placed on the Authorized Personnel List and then every two years thereafter. The Tribe will be required under the new MOU to have the internal security incident handling procedures; more information on the required policies/procedures is available in Section 3.1 and Section 5.2. The LASO must ensure that the training curriculum is adequate and covers the required topics. Training outlines will be reviewed by the NIGC during audits.

As discussed above, the LASO is responsible for maintaining and updating the Training Documentation Form showing that both CJIS Online and tribal internal privacy and security training have been completed. NIGC's compliance training is designed to help the LASO or other designated tribal/TGRA representative understand the new compliance requirements so that they can implement the rules back at their Tribe and TGRA; NIGC training does not take the place of the tribe's internal training. The Tribe/TGRA must document each instance when its Authorized Personnel receive this training and retain documentation for a minimum of two years. Upon request, it must be forwarded to the NIGC. A blank Training Documentation Form is located in Appendix J of this guide and is also available for download at the NIGC website at <https://www.nigc.gov/compliance/CJIS-Training-Materials>.

4.2.2 Acknowledgement Statements

All authorized personnel must sign a statement acknowledging notification of the penalties for misuse of the CJI and CHRI. There is no standard format for the Acknowledgement Statement. It must state at a minimum that the undersigned "acknowledges notification for the penalties for misuse of criminal justice and criminal history record information," but ideally it contains a summary of state, federal, and tribal consequences. TGRAs may choose to add a short training outline to the statement so that the employee specifically acknowledges their training as well.

The LASO is responsible for entering the date Acknowledgement Statements were signed on the Training Documentation form. Do not send the acknowledgement statements to the NIGC; keep the forms on file at the TGRA/tribe. NIGC personnel will review these forms during the tribe's audit.

4.3 Audit Responsibilities

The LASO is the tribe's representative for all audits and cooperates with federal and state officials throughout the audit process. More details on the audit process are contained in Section 5.

The LASO's responsibilities during an audit include:

- Ensuring all the audit instructions are followed and that the audit packet is returned in a timely manner.
- Being present for the audit interview and notifying/gathering any other TGRA/tribal personnel who may be needed to answer the auditor's questions.
- Having all requested documentation available for the audit.
- Serving as the primary coordinator for any corrective actions stemming from the audit findings.

Section 5 - Audits & Compliance

TGRAs who utilize the NIGC fingerprint submission program are subject to an audit by the NIGC and the FBI to ensure compliance with federal rules regarding fingerprint submissions and CJI/CHRI use. The FBI Audits include the Noncriminal Justice Information Technology Security (NCJITS) Audit and the National Identity Services (NIS) Audit. This section explains the general audit process and discusses the FBI CJIS and NIGC requirements. A Compliance checklist and IT checklist can be found in Appendix K.

5.1 Audits

A routine audit cycle has been established for noncriminal justice agencies in order to assess compliance with tribal and federal policies and regulations. For NIGC audits, NIGC personnel will conduct the audits.

5.1.1 Routine Audits

A routine audit is a scheduled review of the Tribe's compliance with the FBI CJIS and NIGC requirements. The NIGC will notify the Tribe approximately 30 days in advance of the planned audit date. The notification will describe the audit process and provide the contact information of the assigned NIGC Compliance Officer. The LASO should contact the NIGC Compliance Officer to acknowledge receipt of the audit notification.

The notification will state whether the Tribe is scheduled for a telephonic or an in-person audit. The LASO must be present for the audit; the Tribe may also have other personnel in attendance if needed or desired. Compliance assessment documents will be sent with the notification; these documents will need to be completed and returned by the date indicated on the accompanying audit timeline.

The NIGC Compliance Officer will conduct a complete file review of the TGRA/tribe prior to the audit interview. All documentation relating to general administration, fingerprint submissions, privacy and security, and training will be reviewed at or before the audit interview. The LASO will be asked to complete an assessment questionnaire and a chart as part of the pre-interview process.

After an audit has been completed, the NIGC Compliance Officer will provide the TGRA/tribe with a written report which will either denote complete compliance or will contain recommendations for corrective actions to bring the TGRA/tribe into compliance. NIGC Compliance Officers are available to discuss specific concerns and to offer training to assist the TGRA/tribe in this process.

5.1.2 Directed Audits

A directed audit is an administrative review prompted as a result of an incident or allegation of possible misuse of CJI/CHRI. Most issues of misuse stem from instances of improper dissemination of criminal history record information to unauthorized individuals or agencies.

The NIGC may conduct a directed audit of a Tribe if the NIGC:

- Receives a complaint from a Tribe or individual alleging misuse of CJI/CHRI.
- Becomes aware of Tribal actions which may constitute a misuse of CJI/CHRI.
- Becomes aware of Tribal actions which may be a violation of the MOU terms.

A NIGC Compliance Officer will contact the tribe's LASO and arrange to conduct a review of the TGRA/tribe's processes and actions which may have resulted in a misuse. If the Compliance Officer cannot reach the LASO within a reasonable period of time, they will contact the LASO's supervisor, authorized tribal official on the MOU, or other administrator.

The review by an NIGC Compliance Officer is designed to detect process issues that may result in noncompliant actions by a TGRA/tribe. Areas audited are the same as those checked during a routine audit, and the review may focus on the policies, procedures, process, and actions most closely related to the allegation. NIGC Compliance Officers will ask questions regarding the circumstances surrounding the allegation to determine if/how the incident occurred and what actions might be required to prevent a repeat of any misuse. The LASO should be present for the audit as well as any other personnel the TGRA/tribe deems necessary. Following the directed audit, the NIGC Compliance Officer will prepare a written report of their findings. If compliance issues are detected, the report will contain recommendations and/or specific requests in order to bring the TGRA/tribe into compliance so that it can continue to utilize the fingerprint criminal history check process through the NIGC. The Tribe will be required to respond in writing regarding its corrective actions in the areas of concern.

A directed audit does not replace a routine audit. If a directed audit finds issues that require correction, a TGRA/tribe may be scheduled for a routine audit after a specified period to reassess its compliance.

5.2 Compliance Review

This subsection discusses the general compliance requirements for each of the areas reviewed by NIGC Compliance Officers: general administration, fingerprint submissions, privacy and security, and training. Each part contains a short explanation of the requirements and may reference different resources or areas of the guide which a TGRA/tribe may refer to for more information.

5.2.1 General Administration

The general administration section of an audit reviews the basic information on file for the TGRA/tribe for completeness, accuracy, and compliance with current regulations.

- 1) Memorandum of Understanding (Section 1.2)
The MOU is the contractual agreement between the tribe and the NIGC that allows the NIGC to provide CJI/CHRI upon submission of fingerprints. Changes to the signatory to the MOU may be a reason that the MOU needs to be updated. The LASO's duties regarding information changes are detailed in Section 4.1.1.
- 2) Authorized Personnel List (Section 4.1.2)
The LASO is responsible for maintaining an updated Authorized Personnel List on file with the NIGC. The Authorized Personnel List contains those individuals whom the TGRA/tribe has identified as authorized to access, handle, and/or destroy CJI/CHRI. The authorizations are based solely on the TGRA/tribe's determination, but must be limited to the minimum number of personnel necessary. **ALL** personnel who view, handle, use, disseminate, or dispose of CJI/CHRI **MUST** appear on the list; the list will be checked at every audit.
- 3) Tribe File Information (Section 4.1.1)
The LASO must inform the NIGC in writing of changes in the authorized tribal signatory on the MOU, the LASO designation, or any relevant business information (tribe name changes, mailing/physical address changes, etc.). The NIGC Compliance Officer will check that all the information on file at the NIGC is current. Make changes as they occur – do not wait for an audit!
- 4) Authorization and Purpose (Section 1.2, Section 1.3, Section 2.13.1 #17)
Each fingerprint submission access is for a specific purpose and is pursuant to a specific authorization. Fingerprints cannot be submitted for any purpose other than that which is named in the tribe's authorization. The NIGC Compliance Officer will check the tribe's authorization

and verify each purpose.

5.2.2 Fingerprint Submissions

The NIGC Compliance Officer will review the tribe's entire fingerprint submission process covering properly filling out the cards, applicant identification, processes to protect the fingerprint card from tampering, and notifications and disclosures to the applicant.

- 1) Proper Citing of the “Reason Fingerprinted” (Section 2.13.1 #17)
Fingerprint cards may only be submitted for specific purposes under approved authorizations. In the “Reason Fingerprinted” box on the card, TGRAs are required to specify the particular purpose for the submission – “Indian Gaming License or Employment of a Key Employee or Primary Management Official”
- 2) Applicant Identification (Section 2.2)
TGRAs must have processes for verifying the identity of the applicant at the time of fingerprinting. The NIGC Compliance Officer will check for procedures, which include:
 - Informing fingerprinting personnel of the identification requirement.
 - Requiring proper identification at the time of fingerprinting.
- 3) Protection of the Fingerprint Card Prior to Submission (Section 2.12)
Agencies must have processes for protecting the integrity of the fingerprint card and preventing tampering with the card from the time the prints are taken through the submission to the NIGC. The NIGC Compliance Officer will look for procedures which establish either a process that prevents the applicant from possessing a completed fingerprint card or prevents direct access to the card (such as a sealed envelope system). The processes must also include instructions to fingerprinting personnel as necessary.
- 4) Review and Challenge Notification (Section 3.3)
It is the TGRA/tribe’s responsibility to notify applicants in writing of the opportunity and ability to review, correct, update, and/or challenge a criminal history record. Also applicants must be provided a reasonable amount of time to do so before a final licensing and/or employment decision is made. Review and challenge contact information is in Section 3.3 of this guide.
- 5) FBI Applicant Privacy Rights Notifications and FBI Privacy Act Statement (Section 2.3)
Any tribe which submits fingerprints for FBI criminal history (federal check) is required to advise applicants of the following PRIOR to submitting the fingerprint card for a criminal history check:
 - Applicants must be notified in writing that their fingerprints will be used to check the criminal history records of the FBI. The written notification to the applicant includes electronic notification.
 - Informing all applicants that they are allowed a reasonable opportunity (this must be defined in a tribal policy, i.e. 5 days) to complete and challenge the accuracy of their criminal history record before a final denial of a license and/or employment.
 - TGRAs must notify applicants in writing how to obtain a copy of the FBI record, how to update, correct, change, or challenge it, and that the guidelines for these procedures are contained in Title 28 C.F.R. § 16.34.

Additionally:

- The TGRA/tribe must also establish and document what constitutes a reasonable period of time for the review and challenge of the criminal history record and any appeals process that is available to the applicant.

- It is highly recommended (but not required) that the written notifications be presented to the applicant on a document that the applicant is required to sign.

5.2.3 Privacy and Security

TGRAs must have written policies and procedures regarding access, use, handling, dissemination, and destruction of CJI/CHRI (See Section 3.1). The NIGC Compliance Officer will review the TGRA/tribe's required privacy and security policies and procedures and any documents/processes related to security and dissemination of CJI/CHRI. Section 3 of this guide covers required policies and basic privacy and security guidelines.

- 1) The TGRA/tribe must have a process which ensures that CJI/CHRI is only used for the purpose for which it is requested. Under IGRA that purpose is licensing and/or employment of key employees and primary management officials of the tribe's gaming enterprise.
- 2) The TGRA/tribe must have processes in place for the proper access and handling of CJI/CHRI.
 - Access includes:
 - Defining who is authorized to access CJI/CHRI
 - Restricting access to only Authorized Personnel
 - Handling rules include:
 - Proper security of CJI/CHRI from receipt through destruction
 - Communication rules
 - Communication among Authorized Personnel
 - Communication with the applicant concerning CJI/CHRI
 - Communication with the NIGC upon discovery of security incidents (within 24 hours)
 - Secondary/Reuse dissemination procedures (if authorized by federal or state law beyond IGRA)
 - As a general matter, secondary dissemination or reuse is not allowed for CJI/CHRI obtained from the NIGC
 - Logging/tracking procedures
 - Procedures for authenticating recipients of the disseminated information
 - Retention procedures
 - Destruction procedures
- 3) The Tribe must have processes in place to prevent the unauthorized disclosure of CJI/CHRI. Prevention of unauthorized disclosure includes:
 - Access-limited storage.
 - Not leaving CJI/CHRI unattended when it is not physically secured.
 - Revocation of access privileges for terminated employees or those removed from the Authorized Personnel List.
- 4) The TGRA/tribe must have a formal disciplinary process in place for misuse of CJI/CHRI. This includes a formal sanctions process for personnel that fail to comply with information security policies and procedures, including those mandated by the CJIS Security Policy.
- 5) If applicable, the TGRA/tribe must have processes in place governing electronic storage of CJI/CHRI. This includes:
 - Monitoring and restricting access to databases containing CJI/CHRI.
 - Physical/technical safeguards to protect the access and integrity of the CJI/CHRI.
 - Reporting, response, and security incident handling capability for information security incidents.

5.2.4 Training

The NIGC Compliance Officer will review the TGRA/tribe's training documentation to verify Authorized Personnel have received both the mandatory CJIS training (or equivalent) and the TGRA/tribe's internal process training. All personnel with access are required to be trained in both.

- 1) All Authorized Personnel must be trained in the online security awareness (CJIS or equivalent) training within six months of hire or of being placed on the Authorized Personnel List and then every two years thereafter.
- 2) All Authorized Personnel must receive the TGRA/tribe's internal training on the access/use/handling/ dissemination/destruction procedures within six months of hire or of being placed on the Authorized Personnel List and then every two years thereafter. The Tribe's training must also cover the federal and tribal consequences for misuse of criminal history. The Compliance Officer will ask to view the TGRA/tribe's training and any reference policies to assess the training topics. (See Section 4.2.1)
- 3) All Authorized Personnel must sign an Acknowledgement Statement acknowledging the notification of the penalties for misuse of CJI/CHRI. There is no standard format for the Acknowledgement Statement, but it must state at a minimum that the individual has been notified of the consequences of misuse of CJI/CHRI. Agencies may choose to summarize the consequences on the Acknowledgement Statement or refer to specific policies or training materials. (See Section 4.2.2)
- 4) Authorized Personnel training must be logged on the NCJA Training Documentation Form (or equivalent) Specifically, the TGRA/tribe must document each instance when its Authorized Personnel receive training and retain documentation for a minimum of two years. The training documents must be available for inspection by FBI and NIGC auditors and Compliance Officers.

5.2.5 Key Employee and Primary Management Official Checklist

This checklist is provided to assist the TGRA/tribe in determining which gaming license or employment applicants' fingerprints can be submitted through the NIGC to obtain a CHRI for eligibility determinations. The checklist will be used by the NIGC during the audit process and the checklist or a similar process should be used by the TGRA/tribe to ensure only those employees who meet the definition of Key Employee and Primary Management official are fingerprinted through the NIGC. Tribal Gaming Commission staff and Gaming Commissioner are not typically employees of the gaming operation therefore they do not meet the definition of Key Employee or Primary Management Official listed below. For more information on the NIGC background and licensing regulations, please visit <https://www.nigc.gov/general-counsel/commission-regulations> parts 556 and 558.

5.2.6 Gaming Operation Definition

25 C.F.R. § 502.10 defines Gaming Operation as the economic entity that is licensed by a tribe, operates the games, receives the revenues, issues the prizes, and pay the expenses. A gaming operation may be operated by a tribe directly; by a management contractor; or, if individually-owned gaming is allowed, by another person or other entity.

5.2.7 Key Employee Definition

Per 25 C.F.R. §502.14 defines Key Employee as:

- (a) A person who performs one or more of the following functions:
Bingo caller, counting room supervisor, Chief of Security, custodian of gaming supplies or cash, floor manager, pit boss, dealer, croupier, approver of credit, or custodian of gambling devices including persons with access to cash and

- accounting records within such devices;
- (b) If not otherwise included, any other person whose total cash compensation is in excess of \$50,000 per year; or,
- (c) If not otherwise included, the four most highly compensated persons in the gaming operation.
- (d) Any other person designated by the tribe as a key employee.

5.2.8 Primary Management Official Definition

Per 25 C.F.R. §502.19 defines Primary Management Official as:

- (a) The person having management responsibility for a management contract;
- (b) Any person who has authority:
 - (1) To hire and fire employees; or
 - (2) To set up working policy for the gaming operation; or
- (c) The chief financial officer or other person who has financial management responsibility.
- (d) Any other person designated by the tribe as a primary management official.

Any Key Employee or Primary Management Official who are classified under 25 C.F.R. 502.14 (d) and 502.19 (d) must have an attribute of 25 C.F.R 502.14 (a-c) or 502.19 (a-c)

A sample Key Employee and Primary Management Official checklist can be found in Appendix L.

Additionally, a Key Employee and Primary Management Official bulletin can be found in Appendix M.

When submitting a Notice of Results (NOR) to the NIGC, the document may contain summary CHRI if specifically referencing the FBI CHRI results. Updating the NOR to remove the FBI CHRI results can help eliminate summary CHRI. A revised sample NOR form can be found in Appendix N.

5.3 National Identity Services Audit

The FBI's CJIS Division has established audit programs for the purpose of evaluating compliance with policy requirements associated with access to CJIS systems and information. The National Identity Services (NIS) Audit assesses compliance with Interstate Identification Index (III) and National Fingerprint File (NFF) participation standards; federal laws and regulations associated with the use, dissemination, and security of national CHRI; and National Crime Prevention and Privacy Compact (Compact) rules and procedures. The NIS Audit is conducted with state criminal history record repositories, federal agencies, FBI-approved channelers, and other entities authorized access to Next Generation Identification (NGI) and III, and includes reviews of local agency components within their applicable jurisdictions.

Agencies which access criminal history records for non-criminal justice licensing and employment purposes must meet requirements established in federal laws and regulations, as well as requirements established by the Compact Council for such access. Specific policies include: Use of CHRI; Reason Fingerprinted Field and Purpose Code Usage; Dissemination of CHRI; Applicant Notification and Record Challenge; Name-Based III Access Using Purpose Codes I and X; User Fee; and Audit Program. Primary sources for these policy requirements include:

- Title 28, U.S.C Section 534 (a)(4) and (b)
- Title 42, U.S.C, Section 14616, Article IV (c) and Article V (a) and (c)
- Title 5, U.S.C., Section 552a, (e)(3)
- Title 28, C.F.R. Section 50.12, (b)
- Title 28, C.F.R., Section 20.33, (a)(3) and (d) • Title 28, C.F.R., Section 901

- III/NFF Operational and Technical Manual, Chapter 2, Section 2
- CJIS Security Policy, Version 5.3, Section 5.11.2

For more information on the NIS Audit, please visit <https://www.fbi.gov/file-repository/national-identity-services-pdf.pdf/view>

5.4 Information Technology Security Audit

The purpose of the audit is to assess the user community's compliance with the FBI CJIS Security Policy requirements as approved by the Advisory Policy Board (APB) and National Crime Prevention and Privacy Compact (Compact) Council. The FBI CJIS Security Policy provides a baseline of security requirements for current and planned services and sets a minimum standard for new initiatives. The FBI CJIS Security Policy applies to all entities with access to, or who operate in support of, FBI CJIS Division's services and information. The FBI CJIS Security Policy provides the minimum security requirements associated with the creation, viewing, modification, transmission, dissemination, storage, and/or destruction of CJI and CHRI. Entities engaged in the interstate exchange of CJI/CHRI data for non-criminal justice purposes are also governed by the standards and rules promulgated by the Compact Council to include the Outsourcing Standard for Nonchannelers.

5.4.1 Noncriminal Justice Audit - an audit of a non-criminal justice agency's access, use, storage, and destruction of any CJI/CHRI received from FBI CJIS systems via direct and indirect access methods. These audits include both name-based and fingerprint-based queries over wired or wireless networks.

5.4.2 Outsourcing/Channeling Audit – an audit of an FBI approved contractor who submits fingerprints on behalf of an authorized recipient to the FBI and receives the results of such a submission for dissemination back to the authorized recipient. The scope of nonchanneler audits focuses mainly on the storage, dissemination, and destruction of CHRI.

These audits are comprised of an administrative interview to review administrative and technical controls that are implemented to protect CJI/CHRI from both a physical and logical perspective. Additionally, most audits include a physical security and network inspection in which controls identified in the administrative interview are verified to be implemented and working correctly. For more information on the Information Technology Security Audit please visit <https://www.fbi.gov/file-repository/information-technology-security.pdf/view>

Section 6 – NIGC Classes & Assistance

The NIGC provides training to noncriminal justice agencies receiving CJI and CHRI. The NIGC's compliance training is designed to help the Local Agency Security Officer (LASO) or other designated tribal representatives understand the compliance requirements so that they can implement the rules back at their Tribe. The NIGC training **does not** take the place of the TGRA/tribe's internal training. It is each TGRA/tribe's responsibility to ensure that its Authorized Personnel are properly trained in the requirements detailed in Section 5.2.4.

6.1 Initial Access & NCJA Compliance Training

All new TGRAs are required to have at least one representative complete Initial Access & NCJA Compliance Training prior to submitting any fingerprint cards. This training is not required for existing TGRAs; however, it is recommended if a TGRA/tribe has experienced personnel turnover or TGRA/tribal personnel wish to attend a refresher in order to ensure compliance with current requirements. The persons who attend training should be prepared to share the information learned with other relevant TGRA/tribal personnel. This training is for the LASO and tribal trainers – this is NOT the training which is required for all Tribe Authorized Personnel. Authorized Personnel training requirements are explained in the class.

Class Description

Initial Access & NCJA Compliance Training lasts approximately six hours and covers the basic rules in this guide and provides information on the following:

- How to properly fill out the information on a fingerprint card.
- Fingerprint submission packet requirements
- How to read and interpret CJI/CHRI.
- Complying with NIGC and federal requirements associated with noncriminal justice fingerprint criminal history checks
- The LASO's role as the primary TGRA/tribal liaison and guidance regarding TGRA/tribal regulatory compliance and required documentation.
- Basic privacy and security guidelines for the access, use, handling, and destruction of criminal history record information.
- The key areas the TGRAs need to consider when developing policies and procedures for criminal history handling.
- How to identify Key Employees and Primary Management Officials of tribal gaming enterprises.
- Authorized personnel training requirements and an overview of CJIS Online Security Awareness training.
- How to achieve compliance with the FBI and NIGC requirements.

6.2 Types of Training Offered by the NIGC

The NIGC offers several methods for completing the Initial Access & NCJA Compliance Training. Trainings will be provided at Regional Training Course (RTC) locations yearly as well as offered as Site Specific Training (SST). Additional resources may be located on the NIGC website at <https://www.nigc.gov/compliance/CJIS-Training-Materials>.

6.3 Requesting Site Specific Training from the NIGC

Site Specific training is offered to the TGRA and tribe at no cost and can be provided by NIGC Regional staff. To request Site Specific Training please complete the training request form located at <https://www.nigc.gov/training/>. NIGC Region staff will work with the Tribe to schedule and provide the training.

6.4 Other Training Options

The TGRA/tribe can develop and utilize their own security awareness training instead of completing the NIGC training to ensure compliance. The NIGC and FBI allow multiple options to meet the training requirements.

Section 7 - First Steps to Achieve Compliance

7.1 How to achieve compliance

The NIGC has created the following guideline to assist TGRAs in ensuring compliance with the FBI CJIS Security Policy and NIGC MOU requirements.

1. Review Memorandum of Understanding with NIGC (10 days)
 - a. Ensure most recent version is in use (current version 2017);
 - b. Ensure current TGRA head or authorized official has executed agreement; and
 - c. Ensure all staff subject to agreement and using CHRICHRICHI has reviewed its contents.
2. Update authorized personnel list (<http://bit.ly/AUserList>): (10 days)
 - a. Designate Local Agency Security Officer (LASO);
 - b. List all personnel with access to FBI CHRI received from NIGC; and
 - c. Send authorized personnel list to NIGC Information Security Officer (ISO) at iso@nigc.gov...
 - d. Maintain up-to-date authorized personnel list on site and on record with NIGC ISO.
3. Complete and document initial CJIS Security Awareness Training within next 6 months via (30 -60 days):
 - a. PowerPoint presentation;
 - b. Video presentation; or
 - c. Online.
4. Begin reviewing resource information (<https://www.nigc.gov/compliance/CJIS-Training-Materials>) (30-60 days):
 - a. National Information Systems (NIS) Resource Guide;
 - b. Criminal Justice Information Services (CJIS) Security Policy
 - c. NIGC Fingerprint site (<https://www.nigc.gov/finance/fingerprint-process>); and
 - d. TGRA internal policies.
5. Complete CJIS IT Questionnaire (<http://bit.ly/CJISITQuestions>) (10 days):
 - a. Determine readiness/compliance level; and
 - b. Begin improving network hardware, software and policy to achieve compliance (6-12 months).
6. Develop/refine written internal TGRA policies to meet CJIS requirements including (6-12) months:
 - a. Use of fingerprint based CHRI;
 - b. Applicants Rights Notice/FBI Privacy Act Notice/Opportunity to Correct/Copy of CHRI;
 - c. Security Awareness Training;
 - d. Incident Response Policy;
 - e. Auditing and Accountability;
 - f. Access Control;
 - g. Identification and Authentication;
 - h. Configuration Management;
 - i. Media Protection;
 - j. Physical Protection;
 - k. System and Communication Protection and Information Integrity;
 - l. Formal Audits;
 - m. Personnel Security; and
 - n. Mobile Devices;
7. Complete and document internal training on TGRA policies (following timeline of Step 6, 30-60 days).
8. Authorized personnel sign training/penalty acknowledgement statements for TGRA policies (following Step 7).

9. Outsourcing Agreements for non-channelers (6-9 months):
 - a. Identify all IT service providers with access to electronic media containing unencrypted FBI CHRI;
 - b. Identify other service providers with unescorted access to physical copies of CHRI (shredding services, storage facilities);
 - c. Submit request letter to FBI Compact Officer for outsourcing contract approval;
 - d. Execute contract;
 - e. Complete 90-day audit of contractor; and
 - f. Provide certification to FBI Compact Officer that contractor meets CJIS Security Policy.
10. Prepare for first annual NIGC audit using site visit checklist (<http://bit.ly/CJISSVCKList>) (on-going).
11. Continue internal auditing/monitoring to maintain compliance with FBI requirements (on-going).
12. Complete biennial training for users and annually for outsourced non-channelers (on-going).

FBI CJIS Auditor will select three to four tribes Summer/Fall of 2021 for testing against full compliance with NIS and CJIS Security Policy standards as they apply to non-criminal justice agencies and the NIGC MOU.

References

The following state and federal sources referenced below contain rules, regulations, and policies governing the use and dissemination of CJI and CHRI for noncriminal justice purposes. Most of these sources can be readily accessed online. This list is not exhaustive. Additional rules may also be contained in the specific authorization which allows the TGRA/tribe to access CJI/CHRI.

Federal References

U.S. Code of Federal Regulations:

<https://www.gpo.gov/fdsys/browse/collectionCfr.action?collectionCode=CFR>

- Title 28 C.F.R. 20 - Subpart C Federal System and Interstate Exchange of Criminal History Record Information
- Title 28 C.F.R. 0.85(j) - FBI authorized to approve procedures relating to the exchange of identification records.
- Title 28 C.F.R. 50.12 - Funds/approval for records exchange; dissemination limitations; required notification; review and challenge

United States Code: <http://uscode.house.gov/search/criteria.shtml>

- Title 5 U.S.C. 552 - Freedom of Information Act
- Title 5 U.S.C. 552a - Privacy Act of 1974 (as amended)
- Title 42 U.S.C. 14616 - Compact Council

Federal Bureau of Investigation: <https://www.fbi.gov>

- National Crime Prevention and Privacy Compact Council Compact Council Library: Resource documents and references by the Compact Council.
- Identity Verification Program Guide: Published by the National Crime Prevention and Privacy Compact Council to aid fingerprint-submitting agencies in developing policy, procedures, and practices for positive identification of applicants.
- Federal Bureau of Investigations Criminal Justice Information Services (CJIS), CJIS Security Policy.

Acronym Glossary

3DES	Triple Data Encryption Standard
AFIS	Automated Fingerprint Identification System
ASCII	American Standard Code for Information Interchange
CHRI	Criminal History Record Information
CJI	Criminal Justice Information
CJIS	Criminal Justice Information Services
CRI	Contributor Agency Identifier
CSA	CJIS Systems Agency
CSO	CJIS Systems Officer
CTA	Central Terminal Agency
DAI	Designation Agency Identifier
DES	Data Encryption Standard
EFTS	Electronic Fingerprint Transmission Specification
ERRT	Ten-print Transaction Error
ESP	IP Encapsulating Payload
FAUF	Federal Applicant User Fee
FBI	Federal Bureau of Investigation
IAFIS	Integrated Automated Fingerprint Identification System (FBI)
IKE	Internet Key Exchange
IPSec	Internet Protocol Security
IT	Information Technology
L2TP	Layer Two Tunneling Protocol
LASO	Local Agency Security Officer
MIME	Multipurpose Internet Mail Extensions
MOU	Memorandum of Understanding
MS-CHAP	Microsoft PPP Challenge Handshake Authentication Protocol
NCIC	National Crime Information Center
NCJA	Noncriminal Justice Agency
NIGC	National Indian Gaming Commission
NIST	National Institute of Standards and Technology
OCA	Originating Agency Case Number
ORI	Originating Agency Identifier
PII	Personal Identification Information
POP3	Post Office Protocol (version 3)
PPTP	Point-to-Point Tunneling Protocol
RTC	Regional Training Course
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transport Protocol
SnF	NIGC's Fingerprint Store and Forward Server
SRE	Submission Results — Electronic
SST	Site Specific Training
TCN	Transaction Control Number
TCP/IP	Transmission Control Protocol / Internet Protocol
TCR	Transmission Control Reference
TOT	Type of Transaction

Appendix A

MEMORANDUM OF UNDERSTANDING BETWEEN THE FEDERAL BUREAU OF INVESTIGATION AND NATIONAL INDIAN GAMING COMMISSION CONCERNING NONCRIMINAL JUSTICE FINGERPRINT SUBMISSIONS

I. PURPOSE

This Memorandum of Understanding (MOU) documents the agreed-upon responsibilities and functions of the parties with respect to the submission of noncriminal justice fingerprints for primary management officials and key employees of Indian **gaming enterprises**, as defined by NIGC regulations, **25 C.F.R. §§ 502.14(a-c) and 502.19(a-c)**.

II. PARTIES

This MOU is between the Federal Bureau of Investigation (FBI), Criminal Justice Information Services (CJIS) Division, and the National Indian Gaming Commission (NIGC), hereinafter referred to as "Parties".

III. AUTHORITIES

The FBI enters into this MOU under the authority of **28 U.S.C. § 534**. The NIGC enters into this MOU under the NIGC's fingerprint collection and background check authorities that include the following: **25 U.S.C. §§ 2706(b)(3), 2706(b)(7), 2706(b)(10), 2708, 2710(b)(2)(F), 2710(c)(1)-(2), 2710(d)(9), 2711(a), 2711(e)**.

IV. BACKGROUND INFORMATION

The Indian Gaming Regulatory Act (IGRA) established federal standards for gaming on Indian lands to protect Indian gaming as a means of generating tribal revenue. 25 U.S.C. § 2702(3). To carry out this purpose, Congress generally authorized the NIGC to "conduct or cause to be conducted such background investigations as may be necessary" and to "promulgate regulations and guidelines as it deems appropriate to implement the provisions of the IGRA. *Id.* § 2706(b)(3), (10). To assist in that role, Congress specifically provided the NIGC with the power to "secure from any department or agency of the United States information necessary to enable it to carry out" those functions. *Id.* § 2708.

The NIGC submits fingerprints of key employees and primary management officials of Indian gaming enterprises as part of the background screening process required by IGA. *See* 25 U.S.C. § 2710(b)(2)(F), (c)(1)-(2), & (d)(1)(A). The NIGC also submits fingerprints and performs background investigations of "each person or entity ... having a direct financial interest in, or management responsibility for" a management contract. *Id.* § 2711(a). The authority to receive criminal history information for key employees and primary management officials of class II and class III gaming enterprises stems from statutory language specifically empowering the NIGC Chair to "consult with appropriate law enforcement officials concerning gaming licenses issued by an Indian tribe" and to facilitate the suspension of gaming licenses when a key employee or primary management official does not meet the statute's suitability standards with regard to an applicant's criminal history. 25 U.S.C. § 2710(b)(2)(F)(ii)(II), (c)(1)-(2), (d)(1)(A)(ii). Likewise, § 2711(e) requires the Chairman to review the criminal history information of persons with a direct or indirect financial interest in management contracts and to disapprove a management contract when one of those individuals "has been or subsequently is convicted of any felony or gaming offense" or where his or her "criminal record if any ... pose[s] a threat to the public interest or to the effective regulation and control of gaming." This, likewise, applies to both class II and class III gaming. *See* 25 U.S.C. § 2711(e)(1)(B); 25 C.F.R. § 533.6(b)(1)(ii), (c).

V. SPECIFIC RESPONSIBILITIES

A. The FBI will:

1. Conduct fingerprint-based criminal history record searches of NIGC submissions and return the results of the checks to the NIGC.
2. Return rejected fingerprint submissions to NIGC. The NIGC is responsible for notifying each subject of deficiencies in the fingerprint submissions that were rejected by the FBI.
3. Bill NIGC for fingerprint submissions in accordance with the terms of the Interagency Agreement between the NIGC and the CJIS Division.
4. Ensure that the NIGC is not charged supplemental fees for resubmissions and reprocessing of illegible (i.e., unclassifiable) fingerprints, provided that the NIGC follows the procedures outlined by the CJIS Division for the resubmission of the fingerprint cards returned to the NIGC. (This waiver is limited to one resubmission per subject.)

B. The NIGC will:

1. Ensure that all fingerprint submissions have been properly and adequately completed.
2. Convert properly submitted fingerprint card submissions into an electronic format and forward them to the FBI via a means acceptable to the FBI.

- 3. Collect and remit the FBI's fee for the processing of the applicant fingerprint submission. (See 83 FR 48335, dated September 24, 2018, or any successor fee schedule.)

VI. EFFECT OF THIS AGREEMENT

- A. This MOU is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law or otherwise against any of the parties, their parent agencies, the United States, or the officers, employees, agents, or other associated personnel thereof. The parties will seek to resolve any disputes regarding this MOU by mutual consideration.
- B. Except as provided in this document, this MOU is not an obligation or commitment of funds, nor a basis for the transfer of funds, but rather is a basic statement of the understanding between the Parties of the matters described herein. Unless otherwise agreed in writing, each Party shall bear its own costs in relation to this MOU. Expenditures by each Party will be subject to its budgetary processes and to the availability of funds and resources pursuant to applicable laws, regulations, and policies. The parties expressly acknowledge that the language in this MOU in no way implies that funds will be made available for such expenditures.
- C. This MOU does not constitute an agreement for any Party to assume or waive any liability or claim under any applicable law.
- D. The information involved in this MOU may identify U.S. persons, whose information is protected by the Privacy Act of 1974 and/or Executive Order 12333 (or any successor executive order). All such information will be handled lawfully pursuant to the provisions thereof.
- E. Each Party will only disclose personally identifiable information (PII) as authorized under applicable system of records notices published in the Federal Register. For purposes of this MOU, PII is defined as "information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric information, etc., including any other personal information which is linked or linkable to a specific individual."
- F. Before using PII shared pursuant to this MOU, the recipient agency will make reasonable efforts to ensure that the information is accurate, timely, relevant, and complete.
- G. In the event that either Party to this MOU becomes aware of any inaccuracies in the information received from the other Party pursuant to this MOU, the information recipient will promptly notify the information provider so that corrective action can be taken.
- H. Each Party will immediately report to the other Party each instance in which information received from the other Party is used, disclosed, or accessed in an unauthorized manner (including any information losses or breaches).
- I. Each Party will provide appropriate training regarding the responsibilities under this MOU to individuals whose information sharing activities are covered by the provisions of this MOU.
- J. Subject to federal law or regulation, either Party or both Parties may audit the handling and maintenance of information relevant to this MOU in electronic and paper recordkeeping systems to ensure that appropriate security and privacy protections are in place.

VII. EFFECTIVE DATE, MODIFICATION AND TERMINATION

This agreement shall be effective when executed by both Parties and will continue in effect until terminated. This agreement may be modified at any time by written consent of both Parties.

This MOU may be terminated with respect to any Party, at any time, upon written notice of withdrawal to the other Party. Any Party desiring to terminate or modify this MOU will provide such written notification to the other Party at least thirty (30) days prior to modification or termination. The Parties intend to review this MOU annually to ensure all provisions are meaningful and current.

The preceding seven sections represent the understanding reached by the Parties.

FEDERAL BUREAU OF INVESTIGATION,


Michael D. DeLeon
Assistant Director

2/10/2020

Date

Criminal Justice Information Services Division

NATIONAL INDIAN GAMING COMMISSION.



1/17/2020
Date

Christinia J. Thomas Acting Chief of Staff

National Indian Gaming Commission

**MEMORANDUM OF UNDERSTANDING
REGARDING THE DISSEMINATION OF CRIMINAL HISTORY RECORD
INFORMATION BY THE NATIONAL INDIAN GAMING COMMISSION**

In order to facilitate the undersigned tribe (Tribe) in determining the suitability of individuals who have applied for positions as key employees or primary management officials in its gaming operation(s), the National Indian Gaming Commission (NIGC) will be obtaining criminal history record information (CHRI) from the Federal Bureau of Investigation (FBI) on these individuals and disseminating such information to the Tribe.

This memorandum sets forth the following conditions under which the NIGC will disseminate the CHRI to the Tribe:

1. Prior to taking an applicant's fingerprints, the Tribe agrees to provide the applicant with a written notification that informs the applicant that: (i) his or her fingerprints will be used to check the criminal history records maintained by the FBI; (ii) he or she has the opportunity to complete or challenge the accuracy of the information contained in the FBI identification record; (iii) the procedures for obtaining a copy of his or her FBI criminal history record are set forth at 28 CFR §§ 16.30 - 16.33, or by visiting the FBI's website at <<http://www.fbi.gov/about-us/cjis/background-checks>>; and (iv) the procedure for obtaining a change, correction, or updating an FBI identification record are set forth at 28 CFR § 16.34. The Tribe understands that if it does not provide the applicant with this written notification, the NIGC will not disseminate the CHRI to the Tribe.
2. The Tribe understands that the FBI has retained the right to approve the dissemination of the CHRI and may, at some future date, prohibit the NIGC from disseminating CHRI. The Tribe further understands that the NIGC will not release any CHRI without first having received all required prior approvals from the FBI and will not release any CHRI when prohibited from doing so by the FBI. The Tribe also understands that the FBI may impose additional restrictions on the dissemination and use of the CHRI (in addition to those imposed by the NIGC), and that the Tribe will be subject to all such additional restrictions.
3. The Tribe agrees that any CHRI disseminated by the NIGC may be used by the Tribe solely for the purpose of determining a particular applicant's suitability for employment in the Tribe's gaming operation(s).
4. The Tribe understands that NIGC disseminations will only contain the CHRI on a particular applicant and will not contain any NIGC recommendations or conclusions. However, the NIGC reserves the right to furnish (to the Tribe) summary memoranda containing the results of the CHRI.
5. The Tribe agrees that any and all CHRI with which it is provided shall be afforded proper security. The Tribe shall ensure that access to all CHRI disseminated by the NIGC, including all summary memoranda, is restricted to tribal personnel directly involved in licensing deliberations. The Tribe agrees to maintain records of the identities of all persons having access to the CHRI and such records shall be furnished to the NIGC upon request.
6. The Tribe agrees that, except in connection with proceedings related to the Tribe's licensing determinations for its gaming employees, neither the CHRI nor any summary memoranda disseminated by the NIGC shall be reproduced, distributed, or introduced in a court of law or administrative hearing, without the NIGC's prior written consent.
7. The NIGC agrees to promptly notify tribal authorities in the event that the NIGC determines that it is necessary to discontinue disseminating CHRI to the Tribe (either in whole or in part) due to the Tribe's failure to comply with the conditions set forth in this memorandum.

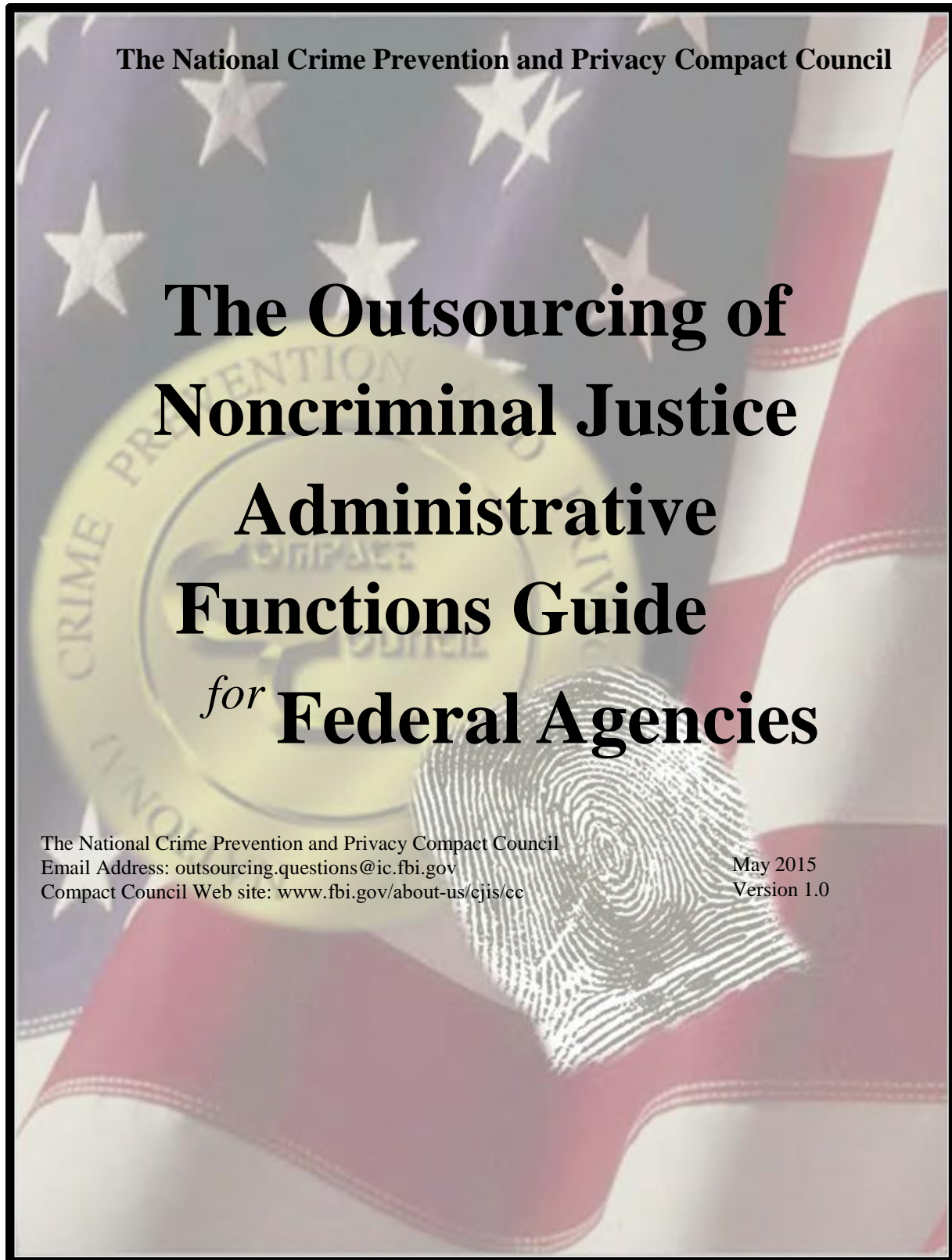
The Tribe acknowledges and consents to the above-stated conditions on this _____ day of _____, 20____.

Name of Tribe

Name of Authorized Tribal Official (PRINT)

Appendix B

The following items are only a select few pages from the full Outsourcing Guide. For the full guide please visit <https://www.nigc.gov/compliance/CJIS-Training-Materials>. Additionally, the Compact Council may update the standards from time to time. Please check with the FBI Compact Officer for most recent guide.



The National Crime Prevention and Privacy Compact Council

The Outsourcing of Noncriminal Justice Administrative Functions Guide *for* Federal Agencies

The National Crime Prevention and Privacy Compact Council
Email Address: outsourcing.questions@ic.fbi.gov
Compact Council Web site: www.fbi.gov/about-us/cjis/cc

May 2015
Version 1.0

Outsourcing: Non-Channeling versus Channeling

There are two very separate and distinct parts to the outsourcing of noncriminal justice administrative functions associated with national criminal history records. The first is Non-Channeling. In this scenario, the Contractor receives access to the CHRI directly from the AR. The AR may engage the Contractor to perform a variety of noncriminal justice administrative functions, such as, but not limited to, obtaining missing dispositions, making fitness determinations/ recommendations, or the off-site storage and archival of fingerprint submissions and corresponding criminal history record results. In this arrangement, the Contractors do not have a direct connection to the FBI's CJIS Wide Area Network (WAN). The AR provides the results of the national criminal history record check directly to the Contractor. The Contractor performs the desired noncriminal justice administrative function(s). Figure 1-1 depicts a Non-Channeling arrangement.

It is important to note that in order to fully comply with footnote 4 of the Outsourcing Standard for Non-Channelers, which provides that if a national criminal history record check of government personnel having access to CHRI is mandated or authorized by a federal statute or executive order approved by the U.S. AG, then the AR must ensure Contractor personnel accessing CHRI are either covered by existing law or that the existing law be amended to include national criminal history record checks for Contractors prior to authorizing the outsourcing initiatives.



The other part of noncriminal justice outsourcing is Channeling, which creates a conduit for an AR to submit fingerprints via an FBI-approved Channeler directly to the FBI, the Channeler receives the CHRI on behalf of the AR, and promptly distributes the CHRI to the AR. The Channeler is a Contractor that has a direct connection to the FBI's CJIS WAN for the electronic submission of fingerprints on behalf of the AR. The FBI electronically returns the corresponding results of each fingerprint-based national criminal history record check to the Channeler and the Channeler expeditiously disseminates the criminal history record check results to the AR. Figure 1-2 illustrates the Channeling arrangement.

In 2011, the FBI released a Request for Proposal (RFP) to solicit Contractors to provide processing services for authorized national noncriminal justice fingerprint submissions from ARs. In response to the RFP, the FBI selected multiple Contractors to act as Channelers. For a current list of Channelers, visit <www.fbi.gov/about-us/cjis/cc/current-initiatives/list-of-fbi-approved-channelers> or contact the FBI Compact Office at <outsourcing.questions@ic.fbi.gov>. Pursuant to the Outsourcing Standard for Channelers, the FBI is required to conduct criminal history record checks of Channeling personnel having access to CHRI. Thus, in this arrangement, the AR is not responsible for conducting background checks of the Contractor's personnel having access to CHRI.

As a matter of information, if the Contractor is posting national criminal history record check results to a Web site, the FBI CJIS Division's Information Security Officer must review and approve the proposed technical configuration prior to the FBI Compact Officer's decision to approve the request.

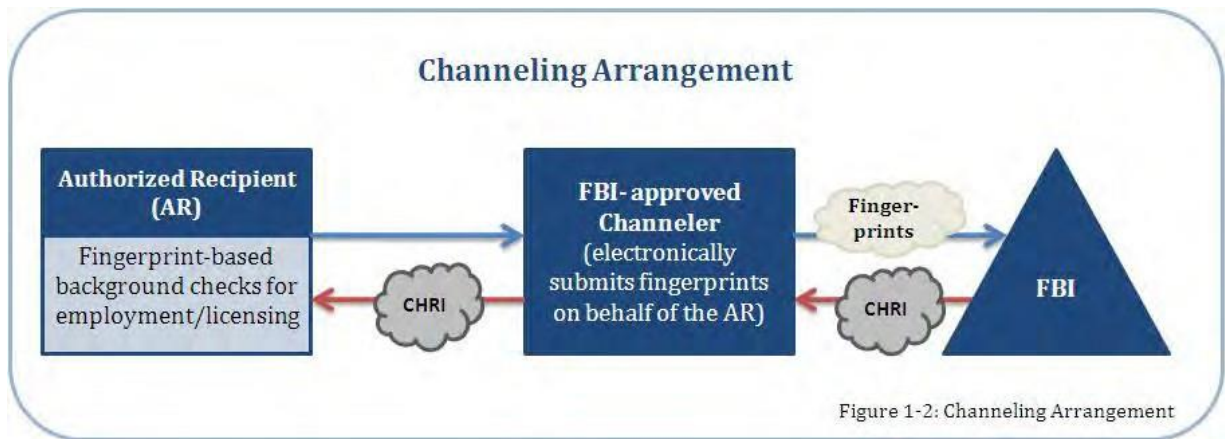


Figure 1-2: Channeling Arrangement

It is possible for the same Contractor to provide both Channeling and Non-Channeling noncriminal justice administrative function services. If this occurs, there must be a distinct separation between the Channeling and the performance of the other noncriminal justice administrative functions (Non-Channeling). A Channeler must promptly forward the criminal history record check results to the AR, which ends the "Channeling" outsourcing process. Then, the AR would be responsible for selecting and forwarding the criminal history record check results back to the Contractor for the performance of approved Non-Channeling noncriminal justice administrative functions, such as obtaining missing dispositions, outsourced by the AR in compliance with the Outsourcing Standard

for Non-Channelers. Such procedures will establish a distinct beginning and end to each of the outsourcing contracts (i.e., a contract for Channeling and a contract for other noncriminal justice administrative functions). Additionally, this process will facilitate an efficient audit process. Essentially, a Channeler is an “expediter” or “conduit” rather than a user of criminal history record results. The Contractor providing the Non-Channeling function is the user of the information. Figure 1-3 displays the same Contractor performing both the Channeling and Non-Channeling functions.

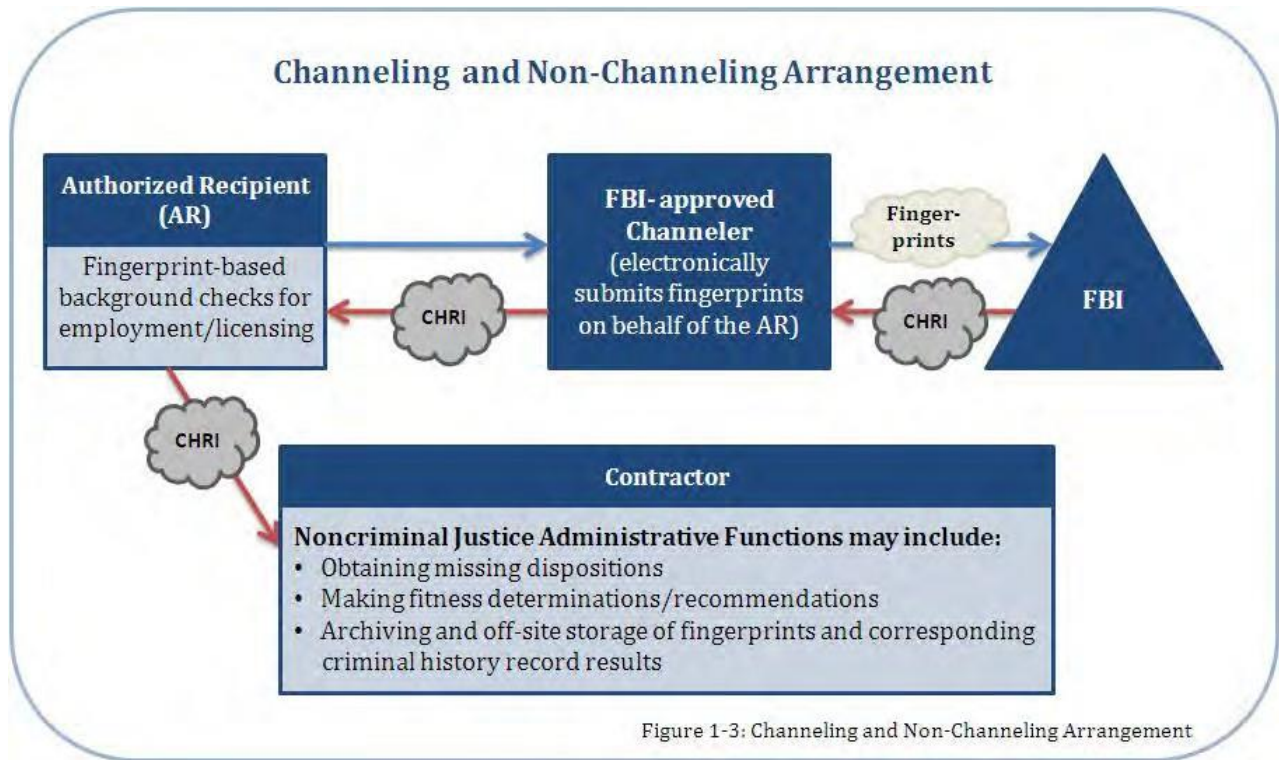


Figure 1-3: Channeling and Non-Channeling Arrangement

Authorized Recipient's Responsibilities

Prior to engaging in the outsourcing of any noncriminal justice administrative functions, the AR is required to request and receive written permission from the FBI Compact Officer. The following sections provide examples of Non-Channeling and Channeling documentation and may be used as a reference when drafting documents relating to the outsourcing of noncriminal justice administrative functions.

Non-Channeling Sample Documentation

- Authorized Recipient Sample Request Letter for Non-Channeling
- Authorized Recipient Sample FBI Response Letter for Non-Channeling
- Sample Language between the Authorized Recipient and Contractor regarding Noncriminal Justice Outsourcing Functions for Non-Channeling

Examples of Non- Channeling Documentation

REQUEST LETTER
FOR THE (Name) **TRIBAL GAMING COMMISSION** TO USE
(Name) **TRIBAL IT DEPARTMENT** AS A CONTRACTOR
FOR NONCRIMINAL JUSTICE ADMINISTRATIVE FUNCTIONS

April 3, 2020

Mrs. Chasity S. Anderson
Compact Officer, FBI Module D3
1000 Custer Hollow Road
Clarksburg, WV 26306

Dear Mrs. Anderson:

The (Name) **Tribal Gaming Commission**, the Authorized Recipient, requests permission to use the (Tribe) **Tribal IT Department** as a contractor to outsource noncriminal justice administrative functions relating to the processing of criminal history record information (CHRI) on its behalf. This would include **[insert all functions that may apply. For example, obtaining missing dispositions, making determinations and recommendations, off-site storage of criminal history record information and its corresponding fingerprint submissions, etc.]** The (Tribe) **Tribal Gaming Commission** and the (Tribe) **Tribal IT Department** are considering entering into an agreement in which (Tribe) **Tribal IT Department** will act on the (Tribe) **Tribal Gaming Commission's** behalf in accordance with the Security and Management Control Outsourcing Standard (Outsourcing Standard) for Non-Channelers. The (Tribe) **Tribal Gaming Commission** is authorized to perform background checks pursuant to Title 25, United States Code (U.S.C.), §2701, et seq, also referred to as the "Indian Gaming Regulatory Act (IGRA)." Specifically, the National Indian Gaming Commission (NIGC) is authorized to submit fingerprints to the FBI on behalf of the (Tribe) **Tribal Gaming Commission** for Class II and III primary management officials and key employees of the Tribal gaming enterprises. "Key employee" and "primary management official" are defined in Title 25, Code of Federal Regulations (C.F.R.), §§502.14 and 502.19 respectively.

The (Tribe) **Tribal Gaming Commission** will execute a contractual agreement with the Contractor, incorporating by reference the Outsourcing Standard for Non-Channelers and the Criminal Justice Information Services (CJIS) Security Policy. Execution of the agreement will commence upon receiving written approval from the FBI Compact Officer and, upon request from the FBI Compact Officer, receipt of a copy of the executed agreement. **The Authorized Recipient shall certify to the FBI Compact Officer that an audit was conducted with the Contractor within 90 days of the date the Contractor first receives CHRI under the approved outsourcing agreement.**

If for any reason the agreement is terminated by either the Authorized Recipient or the Contractor, the Authorized Recipient will provide written notification to the FBI Compact Officer as soon as possible. All records of the Authorized Recipient held by the Contractor will be returned or destroyed, in accordance with the Outsourcing Standard and the CJIS Security Policy, and employees of the Contractor will no longer be allowed access to the CHRI records of the Authorized Recipients.

Upon execution of the Contract, the (Tribe) **Tribal Gaming Commission** will take responsibility for (Tribe) **Tribal IT Department** compliance with the terms of the Contract, to include the Outsourcing Standard for Non-Channelers, and will notify the FBI Compact Officer of any violations.

Sincerely,

[insert name]
[insert title]
[insert address]
[insert phone number]
[insert email address]

cc: iso@nigc.gov

REQUEST LETTER
FOR THE (Name) **TRIBAL GAMING COMMISSION** TO USE
(Contractor's Name) AS A CONTRACTOR
FOR NONCRIMINAL JUSTICE ADMINISTRATIVE FUNCTIONS

April 3, 2020

Mrs. Chasity S. Anderson
Compact Officer, FBI Module D3
1000 Custer Hollow Road
Clarksburg, WV 26306

Dear Mrs. Anderson:

The (Name) **Tribal Gaming Commission**, the Authorized Recipient, requests permission to use the **(Contractor's Name)** as a contractor to outsource noncriminal justice administrative functions relating to the processing of criminal history record information (CHRI) on its behalf. This would include **[insert all functions that may apply. For example, obtaining missing dispositions, making determinations and recommendations, off-site storage of criminal history record information and its corresponding fingerprint submissions, etc.]** The **(Tribe) Tribal Gaming Commission** and the **(Contractor's Name)** are considering entering into an agreement in which **(Contractor's Name)** will act on the **(Tribe) Tribal Gaming Commission's** behalf in accordance with the Security and Management Control Outsourcing Standard (Outsourcing Standard) for Non-Channelers. The **(Tribe) Tribal Gaming Commission** is authorized to perform background checks pursuant to Title 25, United States Code (U.S.C.), §2701, et seq, also referred to as the "Indian Gaming Regulatory Act (IGRA)." Specifically, the National Indian Gaming Commission (NIGC) is authorized to submit fingerprints to the FBI on behalf of the **(Tribe) Tribal Gaming Commission** for Class II and III primary management officials and key employees of the Tribal gaming enterprises. "Key employee" and "primary management official" are defined in Title 25, Code of Federal Regulations (C.F.R.), §§502.14 and 502.19 respectively.

The **(Tribe) Tribal Gaming Commission** will execute a contractual agreement with the Contractor, incorporating by reference the Outsourcing Standard for Non-Channelers and the Criminal Justice Information Services (CJIS) Security Policy. Execution of the agreement will commence upon receiving written approval from the FBI Compact Officer and, upon request from the FBI Compact Officer, receipt of a copy of the executed agreement. **The Authorized Recipient shall certify to the FBI Compact Officer that an audit was conducted with the Contractor within 90 days of the date the Contractor first receives CHRI under the approved outsourcing agreement.**

If for any reason the agreement is terminated by either the Authorized Recipient or the Contractor, the Authorized Recipient will provide written notification to the FBI Compact Officer as soon as possible. All records of the Authorized Recipient held by the Contractor will be returned or destroyed, in accordance with the Outsourcing Standard and the CJIS Security Policy, and employees of the Contractor will no longer be allowed access to the CHRI records of the Authorized Recipients.

Upon execution of the Contract, the **(Tribe) Tribal Gaming Commission** will take responsibility for **(Contractor's Name)** compliance with the terms of the Contract, to include the Outsourcing Standard for Non-Channelers, and will notify the FBI Compact Officer of any violations.

Sincerely,

[insert name]
[insert title]
[insert address]
[insert phone number]
[insert email address]

cc: iso@nigc.gov

Authorized Recipient Sample FBI Response Letter for Non-Channeling

[Date]

[Name] [Position
Title] [Division]
[Federal Agency]
[Address]
[City, State and Zip Code]

Dear [Name]:

Reference is made to your request to use **[insert Contractor's name]** to perform the noncriminal justice administrative functions relating to the processing of criminal history record information (CHRI). This would be limited to **[insert specific noncriminal justice administrative functions to be performed]**. It is noted that your authority for access to the FBI CHRI is **[insert the legal citation of the federal statutory authority or executive order that requires or authorizes the Authorized Recipient to have access to CHRI]**.

In accordance with the National Crime Prevention and Privacy Compact Council's Final Rule entitled "Outsourcing of Noncriminal Justice Administrative Functions," (Title 28, Code of Federal Regulations, Part 906), outsourcing of noncriminal justice administrative functions is permitted under certain conditions when approved by the FBI Compact Officer and as specified in the Security and Management Control Outsourcing Standard for Non-Channelers (Outsourcing Standard).

The **[insert Authorized Recipient's name]** is granted permission to provide CHRI to **[insert Contractor's name]**, as its contractor, solely for the purpose of **[insert specific noncriminal justice administrative functions to be performed]** pursuant to this approval.

In the event of a conflict between the terms of the **[insert Authorized Recipient's name]/[insert Contractor's name]** agreement, amendments to the **[insert Authorized Recipient's name]/[insert Contractor's name]** agreement, and the Outsourcing Standard relating to FBI-provided data, the terms of the Outsourcing Standard shall control.

According to Part 2.05 of the Outsourcing Standard, **[insert Authorized Recipient's name]** shall conduct an audit of the contractor within 90 days of the date the contractor first receives CHRI under the approved outsourcing agreement and shall certify to me that the audit was conducted.

Further, as provided in footnote 2 of the Outsourcing Standard, the FBI will triennially audit a representative sample of contractors and authorized recipients engaging in outsourcing with the first of such audits to be conducted within one year of the date the contractor first receives CHRI under the approved outsourcing agreement. Enclosed is a copy of the most recent version of the Outsourcing Standard, dated November 6, 2014.

Access to the FBI-maintained CHRI is subject to numerous restrictive laws and regulations. Dissemination of such information to a private entity is prohibited except as specifically authorized by federal law or regulation. Further, the exchange of CHRI is subject to cancellation if such unauthorized dissemination is made.

Should you have any questions regarding your responsibilities in relation to the outsourcing of noncriminal justice administrative functions, please do not hesitate to contact [**insert name of CJIS Division POC**] at [**insert telephone number**], or via e-mail at [**insert e-mail address**] or me at [**insert telephone number**], or via e-mail at [**insert e-mail address**].

Respectfully,

[**Insert FBI Compact Officer's name**]
FBI Compact Officer

Enclosure

Note: Send a copy of the response to the Compact Council Chairman and Contractor.

***Sample Language between the Authorized Recipient and Contractor regarding
Noncriminal Justice Outsourcing Functions for Non-Channeling***

CONTRACT BETWEEN
[AUTHORIZED RECIPIENT'S
NAME] AND
[CONTRACTOR'S
NAME] REGARDING
OUTSOURCING
NONCRIMINAL JUSTICE ADMINISTRATIVE FUNCTIONS

This contract is entered into between **[insert Authorized Recipient's name and address]**, the Authorized Recipient, and **[insert Contractor's name and address]**, the Contractor, under the terms of which the Authorized Recipient is outsourcing the performance of noncriminal justice administrative functions involving the handling of criminal history record information (CHRI) pursuant to Title 28, Code of Federal Regulations, Part 906 and the Security and Management Control Outsourcing Standard (Outsourcing Standard) for Non-Channelers. The most current version of the Outsourcing Standard is incorporated by reference into this contract and appended hereto as Attachment "**[insert]**".

The Authorized Recipient's authority to submit fingerprints for noncriminal justice purposes and obtain the results of the fingerprint search, which may contain CHRI, is **[insert the legal citation of the federal statutory authority or executive order that requires or authorizes the Authorized Recipient to have access to CHRI]**. This authority requires or authorizes fingerprint-based background checks of **[insert all categories of current and prospective employees, licensees, or applicants for other benefits covered by federal statutory authority or executive order]**.

The specific noncriminal justice administrative function to be performed by the Contractor that involve access to CHRI on behalf of the Authorized Recipient is to **[insert specific noncriminal justice administrative functions to be performed; i.e., missing dispositions, fitness determinations, storing criminal history record check results]**.

[Insert Contractor's name] will comply with the Outsourcing Standard requirements, to include the *CJIS Security Policy*, and other legal authorities to ensure adequate privacy and security of personally identifiable information and criminal history record check results related to this contract, and will ensure that all such data is returned to the Authorized Recipient as soon as no longer needed for the performance of contractual duties.

NOTE: A copy of the signature page with dates should be included with the contract.

Outsourcing Audit Guidelines

If ARs are authorized to conduct national fingerprint-based background checks based on a federal statute, the FBI Compact Officer may not grant permission to outsource noncriminal justice administrative functions unless he/she has implemented a combined federal audit program to, at a minimum, triennially audit a representative sample of the Contractors and ARs engaging in outsourcing with the first of such audits to be conducted within one year of the date the Contractor first receives CHRI under an approved outsourcing agreement. A representative sample will be based on generally accepted statistical sampling methods.

Additionally, sections 2.05 of the Outsourcing Standards require certification that an audit was conducted with the Contractor within 90 days of the date the Contractor first receives CHRI under the approved outsourcing agreement. It should be noted that each of the Outsourcing Standards places the auditing responsibility on specific parties. Specifically, the FBI will, and the AR may, conduct an audit of the Contractor performing channeling functions and the FBI is required to certify to the FBI Compact Officer that an audit was conducted. The AR will certify to the FBI Compact Officer that an audit was conducted of the Contractor performing Non-Channeling functions.

Sample Audit Methodology

The purpose of the audit is to assess compliance with applicable laws, policies, regulations, and rules which pertain to access to CHRI. The audit should be scoped to cover the following areas:

- adherence to Outsourcing Standard requirements;
- use of CHRI
- dissemination of CHRI
- physical and technical security of CHRI
- compliance with other applicable laws, policies, regulations, and rules.

Agencies are encouraged to use the following sample methodology as a guide when creating the audit process. In addition, Table 2-1 graphically displays the FBI CJIS Division's outsourcing audit methodology. For additional information relating to noncriminal justice agency audits, please refer to the Council's publication *National Criminal History Record Information Audit Guide for Noncriminal Justice Agency Audits*.

Pre-audit

Appropriate representatives from ARs and Contractors selected for audit are identified and notified to discuss an overview of the audit process and scheduling of audit activities. Requests for documentation such as copies of signed contracts occur during this phase. Additionally, points-of-contact are informed that pre-audit materials will be forwarded for review and completion. Pre-audit materials are useful for gathering pertinent information prior to on-site visits and may include high-level questionnaires that are used to formulate specific questions

about agency processes, as well as data quality surveys comprised of a sampling of transactions or records that are used to validate agency processes.

On-Site Audit

Administrative interviews are conducted on-site with appropriate representatives from selected ARs and Contractors. Questions focus on capturing the specific processes used by agencies to meet Outsourcing Standard requirements. In addition, on-site validation of data quality surveys is conducted. Upon completion of the on-site visit, auditors make an initial determination of compliance and conduct an exit briefing with agency personnel. On-site audit activities also include the identification of any follow-up action items necessary to complete assessments.

Report

A draft audit report of findings and recommendations are completed and forwarded to AR and Contractor personnel responsible for oversight and compliance. Findings and recommendations are sufficiently detailed and directly correlate to specific policy requirements. The draft report solicits a response describing corrective actions and offering any additional comments. Upon receipt of the response, the audit report is finalized.

Sanctions

Final audit reports, which incorporate comments from ARs and contractors, are forwarded to the appropriate sanctioning body for review. Upon review, the sanctioning body may consider requiring additional corrective actions or information. In addition, the sanctions process incorporates measures to elevate sanctions in a manner such that deficiencies are corrected and the risk of subsequent violations is adequately mitigated.

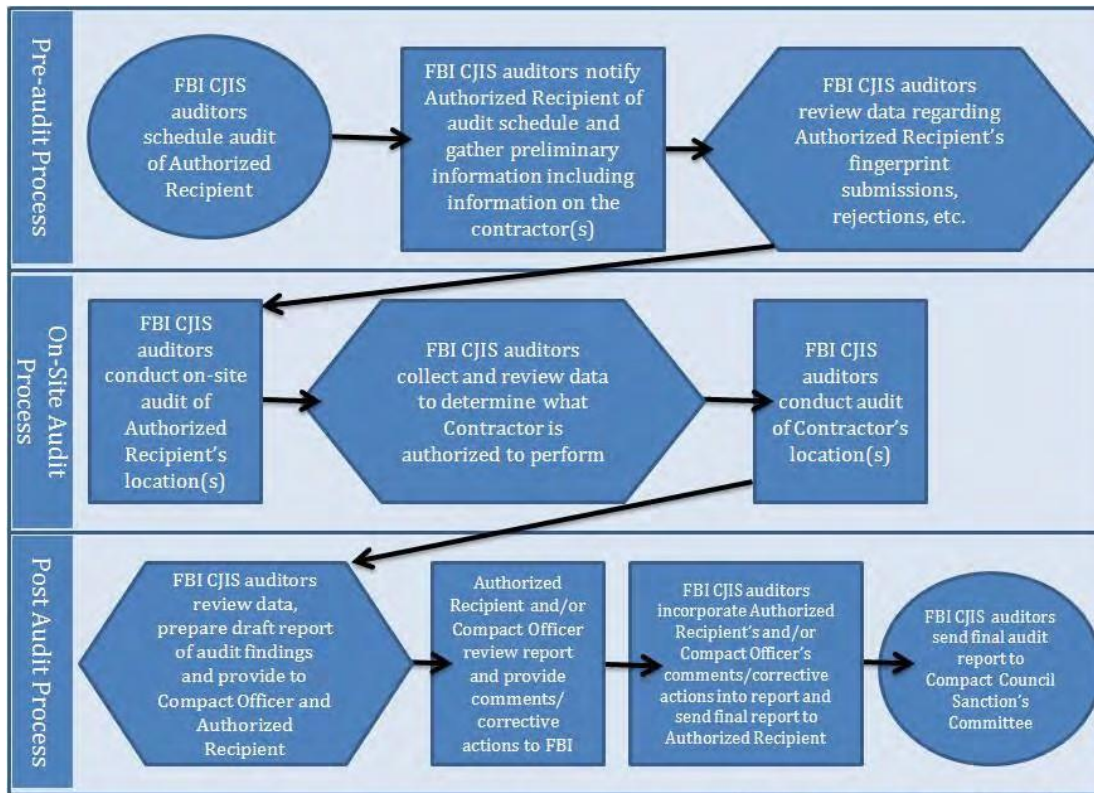


Table 2-1: Outsourcing Audit Methodology

Sample 90 day Audit Checklist for an Authorized Recipient

The Outsourcing Standard for Non-Channelers requires ARs who have been approved to outsource noncriminal justice administrative functions conduct an audit of the Contractor within 90 days of the date that the Contractor first receives CHRI under the approved outsourcing agreement. The following chart has been designed as a tool to assist ARs who are developing an audit process to comply with the 90 day audit requirement based on the Outsourcing Standard for Non-Channelers.

The chart outlines assessment items which have been grouped topically. References to the specific requirements in the Outsourcing Standard for Non-Channelers and the *CJIS Security Policy* have also been provided for each assessment item. Depending on the function outsourced and the specifics of the process, all of the requirements listed may not be applicable.

The chart outlines assessment items which have been grouped topically. References to the specific requirements in the Outsourcing Standard for Non-Channelers and the *CJIS Security Policy* have also been provided for each assessment item. Depending on the function outsourced and the specifics of the process, all of the requirements listed may not be applicable.

Sample 90 day Audit Checklist for an Authorized Recipient

Contractor Assessment	Reference	Yes	No	N/A
	OS-Outsourcing Standard for Non-Channelers CSP-CJIS Security Policy			
Policy References				
a. Copy of current Outsourcing Standard for Non-Channelers	OS 2.02, 2.03, 2.05, 2.07, 3.02, 3.03, 5.03, 6.02, 7.01, 8.01a, 9.01, 9.04, 11.05, 11.06			
b. Copy of current <i>CJIS Security Policy</i>	OS 2.03b, 2.03c, 3.01, 3.02, 3.03, 7.01, 7.02, 9.02			
Security Program				
a. Authorized Recipient (AR) approved minimum requirements for content of Security Program	OS 3.02			
b. Implementation of security requirements	OS 3.02, 3.03 a-d			
c. Reporting procedures for security violations	OS 3.03(c), 8.0			
Security Training Program				
a. AR approved	OS 3.04			
b. Training prior to appointment or assignment	OS 3.04			
c. Training upon receipt of changes	OS 3.04			
d. Annual refresher training	OS 3.04			
Site Security				
a. Available for announced/unannounced audits	OS 3.05			
b. Physically secure location	OS 4.01, 7.02a			
Use and Maintenance of CHRI				
a. Maintained in accordance with contract and does not exceed period of time AR is authorized to maintain	OS 3.07			
b. Used only in accordance with contract and AR's authority	OS 2.03, 3.01			
Dissemination				
a. AR approved in accordance with contract and AR's authority	OS 5.01			
b. Compliant with laws, rules, and regulations[1]	OS 5.01			
c. Log captured required information and retained for a minimum of 365 days	OS 3.08, 5.02			

Personnel Security				
a. Criminal background checks on all Contractor and approved sub-Contractor personnel with access to CHRI conducted prior to access	OS 6.01			
b. Confirmation of understanding by employee(s)	OS 6.02			
c. List of personnel with access to CHRI	OS 6.03			
d. Updates to list of personnel changes within 24 hours of changes	OS 6.03			

Based on OS for Non-Channelers dated 11/06/14 and CJIS Security Policy 5.3 dated 8/4/14

Page 1

[1] Applicable laws, rules, and regulations regarding the dissemination of national CHRI include Title 28, United States Code, Section 534; Title 28, Code of Federal Regulations, Section 50.12 (b) and Part 906.

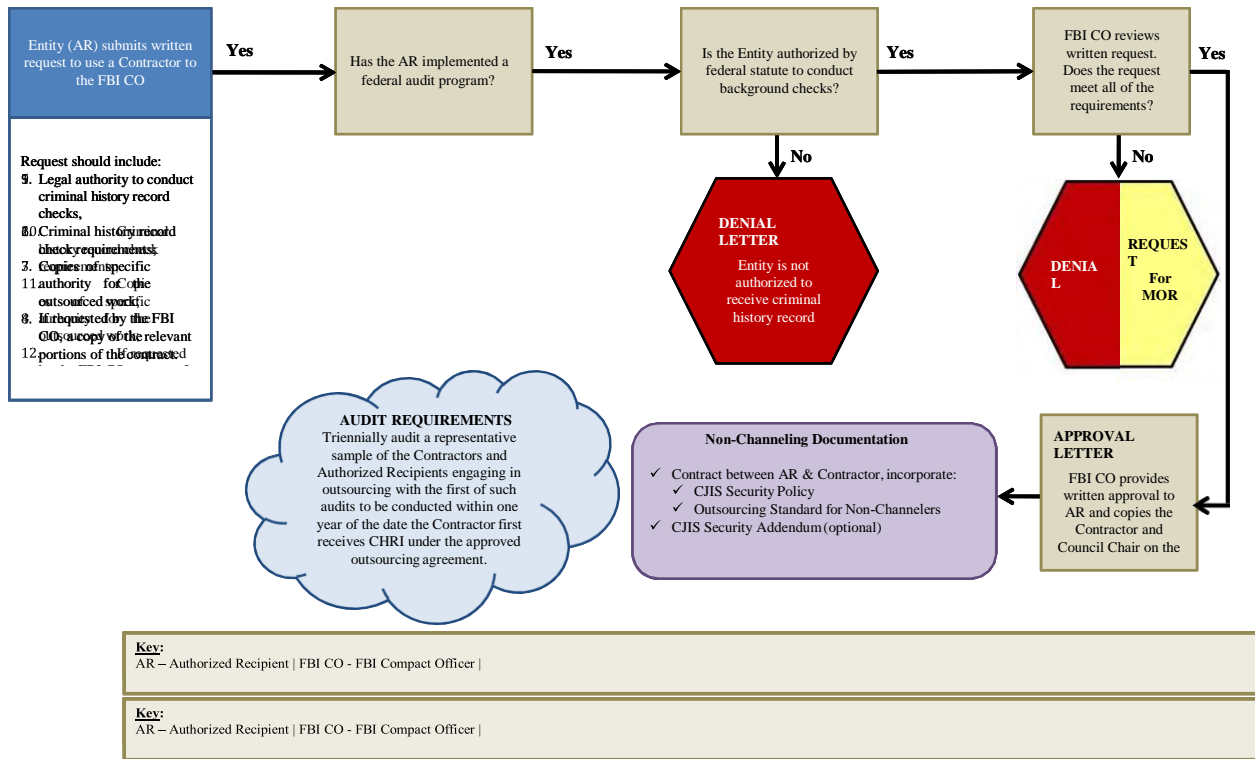
Contractor Assessment	Reference	Yes	No	N/A
	OS-Outsourcing Standard for Non-Channelers CSP-CJIS Security Policy			
Security Violations				
a. Develop and maintain written security violation plan	OS 8.01a, 2.07, 3.03			
b. Policy for disciplinary action	OS 8.01a			
c. Immediate suspension pending investigation	OS 8.01b			
d. Immediate report	OS 8.01c			
d. Follow-up report	OS 8.01c			
Security on Systems Processing CHRI				
a. Current topological drawing	OS 2.04			
b. Firewalls	OS 7.01a, CSP 5.10			
c. Encryption	OS 7.01b, CSP 5.5.2.4, 5.10.1.2			
f. Virus protection on networks processing CHRI	CSP 5.10.4.2			
g. User identification	CSP 5.6			
h. Authentication of user identification	CSP 5.6			
i. Advanced authentication when accessing via the Internet	CSP 5.6			
j. Audit trails	CSP 5.4.6			
Media Destruction				
a. Hard copy	OS 7.02c, CSP 5.8.4			
b. Electronic media	OS 7.02, CSP 5.8.3			

Based on OS for Non-Channelers dated 11/6/14 and CJIS Security Policy 5.3 dated 8/4/14

Page 2 of 2

Non-Channeling Flowchart

Non-Channeling Flowchart



Non- Channeling Checklist

Non-Channeling Checklist

- Must have implemented a federal audit program to, at a minimum, triennially audit a representative sample of the Contractors and ARs engaging in outsourcing with the first of such audits to be conducted within one year of the date the Contractor first receives CHRI under the approved outsourcing agreement.

- Submit the incoming request letter to include copies of the specific authority for the outsourced work, the federal requirement for the criminal history record check, and/or, if requested, a copy of relevant portions of the contract. The legal authority should be referenced in the written request.

- Ensure that the most current versions of both the Outsourcing Standard for Non-Channelers (www.fbi.gov/about-us/cjis/cc/) and the *CJIS Security Policy* (www.fbi.gov/about-us/cjis/cjis-security-policy/cjis-security-policy/view) are incorporated by reference and appended to the contract at the time of the contract and/or option renewal.

- Contract specifies the terms and conditions of CHRI access as specified in the Outsourcing Standard for Non-Channelers and the *CJIS Security Policy*:
 - Limit the use of such information to the purposes for which it is provided
 - Limit the retention of the information
 - Prohibit the dissemination of the information except as specifically authorized by federal laws, regulations and standards as well as rules, procedures and standards established by the Compact Council and the U.S. AG.
 - Ensure the security and confidentiality of the information to include confirmation that the Contractor is authorized to receive CHRI.
 - Provide audits and sanctions
 - Provide conditions for termination of the contract
 - Maintain up-to-date records of contractor personnel that have access to CHRI
 - Ensure contractor personnel comply with the Outsourcing Standard for Non-Channelers and the *CJIS Security Policy*

- Visit the Contractor's facilities for announced and unannounced audits and security inspections.

- Review and approve the Contractor's Security Program.

- Certify that an audit of the Contractor was conducted within 90 days of the date the Contractor first receives CHRI under the approved outsourcing agreement.

Recommended Online Reference Materials

- Security and Management Control Outsourcing Standard for Non-Channelers (current version)–
www.fbi.gov/about-us/cjis/cc/
- FBI *Criminal Justice Information Systems (CJIS) Security Policy* (current version) –
www.fbi.gov/about-us/cjis/cjis-security-policy/cjis-security-policy/view
- FBI Biometric Center of Excellence –
www.fbibiospecs.org
- Electronic Biometric Transmission Specification (EBTS) –
www.fbibiospecs.org/ebts.html

Appendix C

Privacy Act Statement

This privacy act statement is located on the back of the [FD-258 fingerprint card](#).

Authority: The FBI's acquisition, preservation, and exchange of fingerprints and associated information is generally authorized under 28 U.S.C. 534. Depending on the nature of your application, supplemental authorities include Federal statutes, State statutes pursuant to Pub. L. 92-544, Presidential Executive Orders, and federal regulations. Providing your fingerprints and associated information is voluntary; however, failure to do so may affect completion or approval of your application.

Principal Purpose: Certain determinations, such as employment, licensing, and security clearances, may be predicated on fingerprint-based background checks. Your fingerprints and associated information/biometrics may be provided to the employing, investigating, or otherwise responsible agency, and/or the FBI for the purpose of comparing your fingerprints to other fingerprints in the FBI's Next Generation Identification (NGI) system or its successor systems (including civil, criminal, and latent fingerprint repositories) or other available records of the employing, investigating, or otherwise responsible agency. The FBI may retain your fingerprints and associated information/biometrics in NGI after the completion of this application and, while retained, your fingerprints may continue to be compared against other fingerprints submitted to or retained by NGI.

Routine Uses: During the processing of this application and for as long thereafter as your fingerprints and associated information/biometrics are retained in NGI, your information may be disclosed pursuant to your consent, and may be disclosed without your consent as permitted by the Privacy Act of 1974 and all applicable Routine Uses as may be published at any time in the Federal Register, including the Routine Uses for the NGI system and the FBI's Blanket Routine Uses. Routine uses include, but are not limited to, disclosures to: employing, governmental or authorized non-governmental agencies responsible for employment, contracting, licensing, security clearances, and other suitability determinations; local, state, tribal, or federal law enforcement agencies; criminal justice agencies; and agencies responsible for national security or public safety.

As of 03/30/2018

Please ensure the TGRA is using the most update to date Noncriminal Justice Applicant's Rights Notice. To view the recent notice please visit <https://www.fbi.gov/services/cjis/compact-council/guiding-principles-noncriminal-justice-applicants-privacy-rights>

NONCRIMINAL JUSTICE APPLICANT'S PRIVACY RIGHTS

As an applicant who is the subject of a national fingerprint-based criminal history record check for a noncriminal justice purpose (such as an application for employment or a license, an immigration or naturalization matter, security clearance, or adoption), you have certain rights which are discussed below. All notices must be provided to you in writing.¹ These obligations are pursuant to the Privacy Act of 1974, Title 5, United States Code (U.S.C.) Section 552a, and Title 28 Code of Federal Regulations (CFR), 50.12, among other authorities.

- You must be provided an adequate written FBI Privacy Act Statement (dated 2013 or later) when you submit your fingerprints and associated personal information. This Privacy Act Statement must explain the authority for collecting your fingerprints and associated information and whether your fingerprints and associated information will be searched, shared, or retained.²
- You must be advised in writing of the procedures for obtaining a change, correction, or update of your FBI criminal history record as set forth at 28 CFR 16.34.
- You must be provided the opportunity to complete or challenge the accuracy of the information in your FBI criminal history record (if you have such a record).
- If you have a criminal history record, you should be afforded a reasonable amount of time to correct or complete the record (or decline to do so) before the officials deny you the employment, license, or other benefit based on information in the FBI criminal history record.
- If agency policy permits, the officials may provide you with a copy of your FBI criminal history record for review and possible challenge. If agency policy does not permit it to provide you a copy of the record, you may obtain a copy of the record by submitting fingerprints and a fee to the FBI. Information regarding this process may be obtained at <https://www.fbi.gov/services/cjis/identity-history-summary-checks> and <https://www.edo.cjis.gov>.
- If you decide to challenge the accuracy or completeness of your FBI criminal history record, you should send your challenge to the agency that contributed the questioned information to the FBI. Alternatively, you may send your challenge directly to the FBI by submitting a request via <https://www.edo.cjis.gov>. The FBI will then forward your challenge to the agency that contributed the questioned information and request the agency to verify or correct the challenged entry. Upon receipt of an official communication from that agency, the FBI will make any necessary changes/corrections to your record in accordance with the information supplied by that agency. (See 28 CFR 16.30 through 16.34.)
- You have the right to expect that officials receiving the results of the criminal history record check will use it only for authorized purposes and will not retain or disseminate it in violation of federal statute, regulation or executive order, or rule, procedure or standard established by the National Crime Prevention and Privacy Compact Council.³

¹ Written notification includes electronic notification, but excludes oral notification.

² <https://www.fbi.gov/services/cjis/compact-council/privacy-act-statement>

³ See 5 U.S.C. 552a(b); 28 U.S.C. 534(b); 34 U.S.C. § 40316 (formerly cited as 42 U.S.C. § 14616), Article IV(c); 28 CFR 20.21(c), 20.33(d) and 906.2(d).

Updated 11/6/2019

Appendix D

NIGC Fingerprint System Security, Protocols and Data Requirements

System Security

Communication between the Tribe and the NIGC Fingerprint Internet System occurs through the exchange of Internet mail messages over a secure network connection. As mentioned, the Tribe will submit EFTS compliant submissions and receive FBI results using email through a Virtual Private Network (VPN). Agencies will be required to authenticate themselves using strong mechanisms and robust protocols and algorithms to protect the confidentiality and integrity of information being transmitted over the Internet.

The communications system the Tribe will use is the NIGC Internet Security Services (ISS). The ISS provides Group Authentication to the Tribe which is needed to support these enhanced functions. When contacted by the Tribe, the NIGC Fingerprint Administrator will provide to the Tribe the Group Authentication username and password.

The enhanced VPN supported is an end to end SSL Point to Point encryption based on NIST 104-2.

System Protocol(s):

The NIGC's Fingerprint Internet Mail server and the NIGC's AltaScan SnF requires that submitting system(s) send fingerprint submissions using the Simple Mail Transfer Protocol (SMTP). SMTP is a TCP/IP application that allows the transfer of mail from one system to another. The details of this protocol are defined by the following standards:

- 1) RFC 821 – Simple Mail Transfer Protocol (SMTP)
- 2) RFC 822 – Standard for the format of ARPA Internet text messages
- 3) RFC 1652 – SMTP Service extensions for 8-bit MIME transport
- 4) RFC 1521 – MIME Part One: Mechanisms for specifying and describing the format of Internet Message Bodies
- 5) RFC 1522 – MIME Part Two: Message header extensions for NON-ASCII Text

NOTE: The SMTP system must be compatible with the above RFC's.

The body of the SMTP message must be base-64, MIME encoded and single part. The header of the message should include the following parameters:

Date:
From:
To:
Subject:
MIME-Version:
Content-type:

Content-Transfer-Encoding:

The field contents are defined as:

Date: The date and time of which the SMTP message was sent.

From: The mail address, in the form of user@host.domain from which the message was sent. This address will be specified by the NIGC. This will also define the address of the POP3 mailbox to which the NIGC SnF sends the SRE (NIST) responses. This is provided on the Pre-Activation Checklist.

To: The mail address, in the form of user@host.domain, defines where the message will be sent. This is provided on the Pre-Activation Checklist.

Subject: This field contains the message subject. This field should always be set to “Electronic Ten Print Submissions”

MIME-Version: This field specifies the MIME version used to encode the data.

Content-Type: This field specifies the type of body contained in the mail message (application/octet-stream) and an additional attribute for the attachment name (name=efts.sub). The attachment name should be separated by a semi-colon and should always be efts.sub for all 10 print submissions to the NIGC SnF.

Content-Transfer-Encoding: This field specifies the encoding algorithm that was used on the body of the message. This field should always be set to base 64.

When sending a compliant SMTP message, the *typical* SMTP header will look like the following example:

```
Date: Wed May 10 14:25:16 2000  
From: tribe@nigcext01.nigc.gov  
To: triberelay@nigcext01.nigc.gov  
Subject: AltaScan Electronic Ten Print Submissions  
MIME-Version: 1.0  
Content-type: application/octet-stream; name=efts.sub  
Content-Transfer-Encoding: base64
```

Data Requirements:

All Electronic ten-print submissions to the NIGC SnF must be compliant with the ANSI NIST/EFTS 6.2 or EFTS 7.0 standards. The minimum record set includes type 1, 2 and 4 records for each submission. All EFTS mandatory fields must be sent on the submission, (See Tables 1 and 2 for a complete list of descriptors). In addition, the following EFTS fields should contain the provided data elements to meet the NIGC’s requirements:

- 1.04 – TOT The Type of Transaction must be “FAUF” or Federal Applicant User Fee.
- 1.07 – DAI The Designation Agency Identifier (DAI) should contain the value “WVIAFIS0Z”.
NOTE: There is a zero (0) before the Z.
- 1.08 – ORI The Originating Agency Identifier (ORI) should contain “USNIGC00Z”. **NOTE:** There are two zeros (0) before the Z.
- 1.09 – TCN The Transaction Control Number (TCN) must be at least 10 characters and no more than 40 in length with the first 6 characters being the first 6 letters of your Originating Agency Case (OCA) code. **NOTE:** The SnF does not allow any duplicate TCN regardless if the duplicate is from two separate Agencies. If more than one submission with the same TCN is received by the SnF, the second and subsequent submissions will be rejected.
- 1.10 – TCR The Transmission Control Reference (TCR) should contain the IAFIS TCR number if sending a no-charge resubmission. The TCR number is obtained from your IAFIS response. This is the E200... number. The FBI will allow one free resubmission for an applicant. If the resubmission returns an error, the FBI will process the third resubmission as a new submission and bill you. **NOTE:** Leave this field blank if not sending a no-charge resubmission.
- 2.009 – OCA The Originating Agency Case Number must contain the OCA number assigned by the NIGC.
- 2.016 – SSN The applicant’s Social Security Number. **NOTE:** This field is required for the NIGC.
- 2.037 – RFP The Reason Fingerprinted. **NOTE:** This field should contain “Indian Gaming Licensee”
- 2.073 – CRI The Contributor Agency Identifier (CRI) field must also contain “USNIGC00Z”.
NOTE: There are two zeros (0) before the Z.

Table 1. EFTS/NIGC Descriptors

Type 1 NIST Data Descriptors

Identifier	Field Number	Field Name	Character Type	Field Size Per Occurrence		Occurrences		O/M Opt. / Mand.
				Min	Max	Min	Max	
LEN	1.01	Logical Record Length	N	2	3	1	1	M
VER	1.02	Version Number	N	4	4	1	1	M
CNT	1.03	File Content	N	9	48	1	1	M
TOT	1.04	Type Of Transaction	A	4	4	1	1	M
DAT	1.05	Date	N	8	8	1	1	M
PRY	1.06	Priority	N	1	1	0	1	M Default to 2.
DAI	1.07	Destination Agency Identifier	AN	9	9	1	1	M
ORI	1.08	Originating Agency Identifier	AN	9	9	1	1	M
TCN	1.09	Transaction Control Number	ANS	10	40	1	1	M
TCR	1.10	Transaction Control Reference	ANS	10	40	0	1	O
NSR	1.11	Native Scanning Resolution	NS	5	5	1	1	M
NTR	1.12	Nominal Transmitting Resolution	NS	5	5	1	1	M

Items in blue have special NIGC requirements beyond those of the EFTS. (See Section above - Data Requirements)

Table 2. EFTS/NIGC Descriptors Continued

Type 2 NIST Data Descriptors

Data Elements	NIST Field Number	Field Type Alpha Numeric Special	Field Size		Occurrences		O/M Optional/ Mandatory
			Min	Max	Min	Max	
Logical Record Length	2.001	N	2	7	1	1	M
Image Designation Character	2.002	N	2	2	1	1	M
Retention Code	2.005	A	1	1	1	1	M
Attention Indicator	2.006	ANS	3	30	0	1	O
Send Copy To	2.007	ANS	9	19	0	9	O
Originating Agency Case Number	2.009	ANS	9	9	1	1	M
FBI Number	2.014	AN	1	9	0	5	O
Social Security Number	2.016	N	9	9	0	4	M
Miscellaneous Identification Number	2.017	ANS	4	15	0	4	O
Name	2.018	AS	3	30	1	1	M
Aliases	2.019	ANS	3	30	0	10	O
Place of Birth	2.020	A	2	2	1	1	M
Country of Citizenship	2.021	A	2	2	0	1	O
Date of Birth	2.022	N	8	8	1	5	M
Sex	2.024	A	1	1	1	1	M
Race	2.025	A	1	1	1	1	M
Scars, Marks, Tattoos	2.026	AS	3	10	0	10	O
Height	2.027	AN	3	3	1	1	M
Weight	2.029	N	3	3	1	1	M
Eye Color	2.031	A	3	3	1	1	M
Hair Color	2.032	A	3	3	1	1	M
Reason Fingerprinted	2.037	ANS	1	75	1	1	M
Date Printed	2.038	N	8	8	1	1	M
Employer and Address	2.039	ANS	1	120	0	1	O
Occupation	2.040	ANS	1	50	0	1	O
Residence of Person Fingerprinted	2.041	ANS	1	120	0	1	O
Military Code	2.042	A	1	1	0	1	O
Image Capture Equipment	2.067	ANS			0	1	O
Make			1	25	1	1	M
Model			1	25	1	1	M
Serial No.			1	50	1	1	M
Request for Rap Sheet	2.070	A	1	1	0	1	O
Controlling Agency Identifier	2.073	ANS	9	9	1	3	M
Amputated or Bandaged	2.084	C			0	9	Condit.
Finger Number		N	2	2	1	1	M
Amp/Ban Code		A	2	2	1	1	M

Appendix E

CJIS Name Check Request

Please Type or Print Clearly

Please complete the attached form to request a name check. Please be advised that an individual's fingerprints must be rejected twice for technical issues prior to requesting a name check.

*ORI of State/Federal/Regulatory Agency: USNIGC00Z

*Your agency's Point of Contact (POC) for the response: Seneca Chavis

*Phone number of POC: 202-632-0298

*Fax number of POC: 202-606-4935

*Name and Address of requesting agency:

NIGC

90 K Street, N.E., Ste. 200

Washington, DC 20002

C/O Department of the Interior 1849

C Street N.W.

Mail Stop #1621 Washington,

D.C., 20240

Response will be faxed.

*Please complete all the below fields.

Subject of Name Check

Two Transaction Control Numbers (TCN, E#'s) of the subjects fingerprint submission:

(1) E2020

(2) E2020

*Name: _____ *Alias: _____

*Date of Birth: _____ Place of Birth: _____ Sex: _____ Race: _____

*Social Security Number: _____ Miscellaneous Number: _____

State Identification Number: _____ OCA: _____

Please note the asterisked fields are required for Name Check searches, all other fields are optional. Results provided will be the results of biographical information included in the original fingerprint submission.

Appendix F

Example Noncriminal Justice Agency Policies and Procedures

Revised June 20, 2018

Note: Please read these policies in their entirety. You cannot simply copy and paste your Tribe name on these policies for them to be complete or accurate. You must also customize these policies to reflect your Tribe-specific procedures. Everything listed here will be verified during the audit process.

As a guideline, text that is highlighted in yellow is where you enter your Tribe name.

Text that is highlighted in green is either instructions for you or a decision that you must make to reflect your policies. Remove/modify the applicable text from the final document as needed.

GENERAL ADMINISTRATION

I. Purpose

Tribe Name may use the Criminal Justice Information (CJI) or Criminal History Record information (CHRI) obtained from the Arizona Department of Public Safety (DPS) only for the specific purpose of evaluating **(state the purpose from your user agreement - i.e. employees, volunteers, contractors, licenses, etc.)**. CJI/CHRI may not be reused for any other purpose.

II. Authority

Tribe Name has the authorization to submit fingerprints to the National Indian Gaming Commission for Federal Criminal History Checks pursuant to **(list your authority here (i.e. specific Arizona state law, executive order, local ordinance, tribal resolution, etc.))**. The authority is listed in the Noncriminal Justice User Agreement between the National Indian Gaming Commission and **Tribe Name**.

III. Local Agency Security Officer (Primary Liaison)

Tribe Name's Local Agency Security Officer (LASO) is the point of contact with the NIGC through which all communication with the NIGC regarding audits, Tribe/personnel information changes and training and security are conducted. The LASO will maintain all authorized personnel training on the NCJA Training Documentation Form (or similar document). This information will be available at time of audit. The LASO can receive and disseminate communication updates from the NIGC. For the responsibilities of the LASO, refer to the Local Agency Security Officer Basic Responsibility worksheet in the training handouts.

IV. Authorized Personnel

Tribe Name's Gaming Commission (GC) staff may encounter CJI/CHRI. Authorized personnel will be given access to view and handle the CJI/CHRI after completing the required training (CJIS Online Security & Awareness training and reading our Tribe- specific policies and procedures) and the one-time signing of an acknowledgement statement. The Authorized Personnel consists of **(list specific job titles or departments here as needed)**, and designated Local Agency Security Officer (LASO). Refer to the Authorized Personnel List for the most current authorized personnel. The authorized personnel are aware of the other personnel on this list. Upon termination of authorized personnel, the LASO will update the Authorized Personnel List with the NIGC as soon as possible.

The personnel listed on the current Authorized Personnel List on file with the NIGC **Access Integrity Unity (AIU)** are the only personnel authorized to access, discuss, use, handle, disseminate, file, log and destroy the CJI/CHRI. To prevent tampering, all terminated personnel, the public, all outside persons and entities are prohibited from handling or having any access to CJI/CHRI for any reason. Secondary dissemination to an outside agency is prohibited.

If your Tribe does not store CJI/CHRI electronically then remove this entire highlighted paragraph. Only authorized personnel have access to the electronic secured and encrypted database where brief information of the CJI/CHRI are electronically stored. To prevent tampering or unauthorized access, once the authorized personnel is done entering or reviewing information, they must lock the database and log off the computer. Refer to the Storage of CJI/CHRI section below for more information regarding electronic storage. Remove the previous sentence if you do not list more information in the Storage of CJI/CHRI section.

Tribe Name does not store CJI/CHRI electronically.

To prevent unauthorized access or tampering, the fingerprint filing cabinet and drawers are locked throughout the day and one key is secured with the LASO and one other key is secured with the designated authorized personnel. All visitors to the area where CJI/CHRI are kept are accompanied by authorized staff personnel as well.

The Non-Criminal Justice Applicant Fingerprint Card Inventory Sheet(s) must be retained for auditing purposes. The National Indian Gaming Commission is on a three-year auditing cycle and can request to see the previous year's inventory sheets. For example, if the audit is being conducted in 2018, the inventory sheets from 2017 must be made available if requested.

Where possible, have personnel on the Authorized Personnel List been fingerprinted? As there is no Arizona state law existing as a specific authorization, this is not currently required. State if you are able to do this however. For example, many agencies in this program have a user agreement that states the purpose is for employment. In this example you could fingerprint the personnel on your list. If your purpose is adoption certification, then obviously you could not fingerprint the personnel on your list. Personnel with a felony conviction should not have access to CJI/CHRI.

FINGERPRINT SUBMISSIONS

v. Fingerprint Card Processing

Tribe Name requires that all applicants must provide a valid, unexpired form of government-issued photo identification during the application process and prior to fingerprinting to verify their identity. Accepted forms of primary and secondary identification have been approved through the National Crime Prevention and Privacy Compact Council Identity Verification Program Guide.

A copy of the applicant's FBI Privacy Rights Notification will be provided to the applicant prior to fingerprinting.

Tribe Name requires that all applicants must be fingerprinted if they are **(state the purpose from your user agreement - i.e. employees, volunteers, contractors, licenses, etc.)**. Applicants that have disclosed a conviction will be fingerprinted as well. **Applicants are fingerprinted on-site at the Tribe Name's Gaming Commission office or the fingerprint card is given/mailed to the applicant to take to their local police department to get fingerprinted.**

If you mail fingerprint cards to applicants you need to include a chain of custody form so that the fingerprinter can verify the applicant's identity at the time of fingerprinting. A sample form can be found in the NCJ Agency Guide Appendix A. The fingerprinter should be sealing the envelope the fingerprints are mailed in so that the applicant cannot tamper with them. State here if you are doing this and how.

Tribe's Name designated Gaming Commission staff takes possession of the fingerprint card and will ensure the correct purpose and authority (see above) are written on the fingerprint card in the "reason fingerprinted" box. Once the fingerprint card is completed and at no point in time is the fingerprint card to be returned to the applicant. Chain of custody procedures are maintained to protect the integrity of the applicant's fingerprints prior to submission to the NIGC and/or the FBI.

The fingerprint cards are then placed in a manila folder and then into a locked drawer to be mailed with the inventory sheet to the NIGC. Only authorized personnel have access to this locked drawer and the key is stored in the LASO's office.

When a fingerprint card is mailed or provided to the applicant, authorized personnel or designated Gaming Commission staff will provide a packet that contains the following:

- Pre-filled fingerprint card with the employer's address, reason for fingerprint (authorization and purpose) and OCA number.
- A sealable envelope pre-labeled with the employer's address and a space marked with an X on the back of this envelope for the fingerprint technician to sign on the line provided.
- Applicant FBI Privacy Rights Notification.
- Instructions for the applicant on how to handle and return the fingerprint card in the provided envelope.
- Fingerprint technician instructions.

If the envelope shows evidence of opening or tampering, the applicant will be asked to provide another fingerprint card and authorized personnel will repeat the procedures to issue a new fingerprint card.

If your Tribe performs its own fingerprinting then delete this paragraph. If your Tribe sends applicants off-site to be fingerprinted, ensure you state here what your procedures are for ensuring the fingerprinter is verifying the identity of the applicant and how the fingerprints are being safeguarded until they are returned to your Tribe prior to submission to DPS. Does the fingerprinter mail the fingerprints to your Tribe or do they give them back to the applicant?

PRIVACY & SECURITY

VI. Handling/Retention of CJI/CHRI

The fingerprint results from the NIGC are delivered in a sealed envelope clearly labelled “National Indian Gaming Commission”. This mail should be considered to contain CJI/CHRI and should only be provided directly to authorized personnel or the LASO. Only authorized personnel will open mail that contains the CJI/CHRI.

During the course of suitability determination, here are the steps that authorized personnel will follow:

- **If your Tribe does not store CJI/CHRI electronically then remove this bullet point. A summary of the CJI/CHRI are stored electronically on the Gaming Commission secured and encrypted drive with only authorized personnel having access.**
- Before suitability is determined, the CJI/CHRI is stored in a locked drawer for the authorized personnel to review and make a suitability determination.
- After suitability is determined, the CJI/CHRI is stored in a separate employee fingerprinting file. These records cannot be released for any public records request.
- After the final determination is rendered, the CJI/CHRI are filed in the fingerprint filing cabinet which is locked throughout the day and all visitors to the area are accompanied by designated Gaming Commission staff or authorized personnel.

State here if your Tribe retains CJI/CHRI and for how long. If you are not retaining CJI/CHRI state that it is destroyed after a hiring decision or after any appeals process has been completed.

VII. Communication

Authorized Personnel may discuss the contents of the CJI/CHRI with the applicant in a private secure place and extreme care should be taken to prevent overhearing, eavesdropping or interception of communication. The applicant may not be given a copy of the record or allowed to take a picture of it with an electronic device. The record is for **Tribe Name's** use only.

Employees will not confirm the existence or non-existence of an individual's criminal history record to the public or to any unauthorized individual. The applicant should be informed that if he/she wishes to challenge the content of the record, they can contact:

- For a copy of an FBI criminal history record contact the FBI at 304-625-5590. More information can be found at <https://www.fbi.gov/services/cjis/identity-history-summary-checks>

Tribe Name provides all applicants the right to review and challenge his/her criminal history record if they deem the information has been inaccurately reported. Each applicant will be provided **(let applicants know how many days you are providing them to challenge their record)** upon notification to provide **Tribe Name** authentic documentation that reports the criminal history information accurately and completely. This information must be provided prior to determination of suitability for **(state the purpose from your user agreement - i.e. employees, volunteers, contractors, licenses, etc.)**.

CJI/CHRI shall not be copied, emailed, faxed or scanned nor disseminated to secondary parties or the employee. Any casual unauthorized release of information is not allowed (i.e. social media, discussion with friends or family members). CJI/CHRI shall only be discussed (written or verbally) between the authorized personnel as necessary to carry out the specific purpose for which the information was requested and all verbal discussions take place in private.

If the fingerprint-based check has a disqualifying factor, the authorized personnel who opened and reviewed the record will hand-carry the record to the ASC or occasionally other authorized personnel, to determine the next steps. The ASC or authorized personnel will discuss the contents of the record with the applicant in a private and secure manner to obtain any additional information.

If your Tribe does not have an appeals process for an initial denial of employment, etc. then remove this paragraph. **Tribe Name** will provide applicants with an appeals process. The appeals process can take place when the applicant challenges his/her suitability determination made by those on the authorized personnel list. This process concludes with the **(title of individual)** making the final suitability determination.

VIII. Storage of CJI/CHRI

Once the CJI/CHRI has met its purpose, it is filed by authorized personnel in a secured locked filing cabinet in the Gaming Commission office in a secure location. CJI/CHRI are retained in accordance with **Tribe Name's** record retention policy. This CJI/CHRI filing cabinet does not contain any other employment records or any files which may be considered public record to prevent unauthorized access or dissemination. The filing cabinet is locked throughout the day to prevent unauthorized access by non-authorized personnel. The keys to the filing cabinet are kept secure by the LASO and another back-up key is kept secure with other authorized personnel. Only authorized personnel are allowed access to the filing cabinets that contain the CJI/CHRI. If a key to the filing cabinet that contains the records is lost, the filing cabinet will be re-keyed to prevent unauthorized access.

Authorized personnel are responsible for safeguarding the confidentiality of the information at all times and may not disclose or allow access to the information to anyone except authorized

personnel. CJI/CHRI is always secured and never left unattended.

If your Tribe does not store CJI/CHRI electronically then remove this paragraph. The actual copy of the CJI/CHRI results are not electronically stored, but as mentioned above in section VI. Handling/Retention of CJI/CHRI, some essential information is entered for reference and tracking purposes and electronically stored. Physical protection of CJI/CHRI as well as a physically secure location for CJI/CHRI will be shared and verified with the DPS. The database where the CJI/CHRI is stored is in the **Tribe Name Gaming Commission server** which is secure, encrypted and controlled directly by **Tribe Name**. No other organization has access to this database. All visitors to the area where CJI/CHRI are stored electronically are accompanied by authorized personnel.

IX. FBI notifications

The authorized personnel will provide a copy of the FBI Applicant's Privacy Rights Notification to the applicant when they arrive to be fingerprinted. Copies of the FBI Applicant's Privacy Rights Notification are available at the front desk and it will contain the following information:

- Your fingerprints will be used to check the criminal history records of the FBI. If you have a criminal history record, the officials making a determination of your suitability for the job, license, or other benefits must provide you the opportunity to complete or challenge the accuracy of the information in the record. You should be afforded a reasonable amount of time **(your Tribe must define what reasonable means, i.e. 5 days, etc.)** to correct or complete the record (or decline to do so) before officials deny you the job, license, or other benefits based on information in the criminal history record.
- The procedures for obtaining a change, correction or updating of your FBI criminal history record are set forth in Title 28 Code of Federal Regulations, section 16.30 through 16.34. Information on how to review and challenge your FBI criminal record can be found at www.fbi.gov under Identity History Summary Checks or by calling 304-625-5590.

X. Disposal of CJI/CHRI

When the CJI/CHRI has met the destruction date in accordance with **Tribe Name's** record retention policy, authorized personnel will destroy the CJI/CHRI. **State how you destroy CJI/CHRI (either shredding or burning).**

In the event of a third-party contractor that performs the shredding, authorized personnel will accompany the vendor to oversee the shredding and handling of the CJI/CHRI. The authorized personnel, will observe the contractor from the time the shredding receptacle is picked up through the complete destruction of the CJI/CHRI.

XI. Misuse of CJI/CHRI

In the event of deliberate, reckless or unintentional misuse of CJI/CHRI, the employee will be disciplined in accordance with the signed acknowledgement statement and **Tribe Name's**

Gaming Commission policy which can include termination.

XII. Training and Acknowledgement Statements

All authorized personnel must be trained in the online security awareness (CJIS Online) training within six months of hire (or upon being added to the Authorized Personnel List) and then every two years thereafter.

All authorized personnel must be trained in all in-house privacy and security training on the access, use, handling, dissemination and destruction procedures regarding CJI/CHRI within six months of hire (or upon being added to the Authorized Personnel List) and then every two years thereafter.

All authorized personnel will sign an acknowledgement statement regarding the notification of the penalties for misuse of CJI/CHRI.

All training and acknowledgement statements will be recorded on a training documentation log. This log is reviewed during audits by the NIGC.

Acceptable Use Policy

1.0 Overview

The intention for publishing an Acceptable Use Policy is not to impose restrictions that are contrary to <Agency Name> established culture of openness, trust, and integrity. <Agency's Security Team> is committed to protecting <Agency Name>'s employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. Internet/Intranet/Extranet related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, File Transfer Protocol, and National Crime Information Center access are the property of the <Agency Name>. These systems are to be used for business purposes in serving the interests of the agency in the course of normal operations. Effective security is a team effort involving the participation and support of every <Agency Name> employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at <Agency Name>. These rules are in place to protect the employee and <Agency Name>. Inappropriate use exposes <Agency Name> to risk including virus attacks, compromises of the network systems and services, and legal issues.

3.0 Scope

This policy applies to employees, contractors, consultants, temporary staff, and other workers at <Agency Name>, including all personnel affiliated with NCIC and third parties. This policy applies to all equipment that is owned or leased by <Agency Name>.

4.0 Policy

4.1 General Use and Ownership

1. While <Agency Name's> network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of the <Agency Name>. Because of the need to protect <Agency Name's> network, management cannot guarantee the confidentiality of information stored on any network device belonging to <Agency Name>.

2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should consult their supervisor or management.
3. <Agency Name> security department recommends that any information that a user considers sensitive or vulnerable (etc. residual NCIC information on a computer terminal that has access to the internet and CJIS information) be encrypted. For guidance on information classification, see <Agency Name> Information Classification Policy.
4. For security and network maintenance purposes, authorized individuals within <Agency Name> may monitor equipment, systems and network traffic at any time, per <Agency Name> Audit Policy>.
5. <Agency Name> reserves the right to audit the network and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or non-confidential, as defined by agency confidentiality guidelines. Examples of confidential information include, but are not limited to: NCIC information, state criminal history information, agency personnel data, etc. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. Please review <Agency Name's> Password Policy for guidance.
3. All personal computers, laptops, and workstations should be secured with password-protected screen savers with an automatic activation feature, set at ten minutes or less, or by logging off (control-alt-delete) when the computer is unattended.
4. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with "Laptop Security Policy".
5. All devices used by employees that are connected to the <Agency Name> Internet/Intranet/Extranet, whether owned by the employee or <Agency Name>, shall be continually executing approved virus-scanning software with a current database.

6. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4.3 Unacceptable Use

The following activities are, in general, prohibited. Under no circumstances is an employee of <Agency Name> authorized to engage in any activity that is illegal under local, state, federal, or international law utilizing <Agency Name> owned resources. The list below are by no means exhaustive, but attempts to provide a frame work for activities which fall into the category of unacceptable use.

4.4 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Unauthorized access, copying, or dissemination of classified or sensitive information (e.g., NCIC information, state criminal information, etc.).
2. Installation of any copyrighted software for which <Agency Name> or end user does not have an active license is strictly prohibited.
3. Installation of any software without preapproval and virus scan is strictly prohibited.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, logic bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others.
6. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For the purpose of this policy, “disruption” includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
7. Port scanning or security scanning is expressly prohibited unless prior notification has been given to <Agency Name> Security administration.
8. Executing any form of network monitoring which will intercept data not intended for the employee’s host, unless this activity is a part of the employee’s normal job/duty.
9. Circumventing user authentication or security of any host, network, or account.

10. Interfering with or denying service to any user other than the employee's host.
11. Using any program/script/command or sending messages of any kind, with the intent to interfere with or disable a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
15. Providing information about NCIC or list of <Agency Name> employees to parties outside <Agency Name>.

5.0 Enforcement

Violations of this policy include, but are not limited to: accessing data to which the individual has no legitimate right; enabling unauthorized individuals to access data; disclosing data in a way that violates applicable policy, procedures, or relevant regulations or law; inappropriately modifying or destroying data; inadequately protecting restricted data. Any violation of this policy may result in network removal, access revocation, corrective or disciplinary action, civil or criminal prosecution, and termination of employment.

DISCIPLINARY POLICY

In support of *[Agency Name]*'s mission of public service to the city of/county of *[city or county name]* citizens, the *[Agency Name]* provides the needed technological resources needed to personnel to access FBI CJIS systems and information in support of the agency's mission. All agency personnel, with access to FBI Criminal Justice Information (CJI) or any system with stored FBI CJI, have a duty to protect the system and related systems from physical and environmental damage and are responsible for correct use, operation, care and maintenance of the information. All technology equipment: computers, laptops, software, copiers, printers, terminals, MDTs, mobile devices, live scan devices, fingerprint scanners, software to include RMS/CAD, operating systems, etc., used to process, store, and/or transmit FBI CJIS is a privilege allowed by *[Agency Name]*, state CSO, and the FBI. To maintain the integrity and security of the *[Agency Name]*'s and FBI's CJIS systems and data, this computer use privilege requires adherence of relevant federal, state and local laws, regulations and contractual obligations. All existing laws and *[Agency Name]* regulations and policies apply, including not only those laws and regulations that are specific to computers and networks, but also those that may apply to personal conduct.

Misuse of computing, networking or information resources may result in temporary or permanent restriction of computing privileges up to employment termination. In some misuse situations, account privileges will be suspended to prevent ongoing misuse while under investigation. Additionally, misuse can be prosecuted under applicable statutes. All files are subject for search. Where follow---up actions against a person or agency after an information security incident involves legal action (either civil or criminal), the evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s). Complaints alleging misuse of *[Agency Name]*'s computing and network resources and FBI CJIS systems and/or data will be directed to those responsible for taking appropriate disciplinary action.

Examples of Misuse with access to FBI CJI

1. Using someone else's login that you are not the owner.
2. Leaving computer logged in with your login credentials unlocked in a physically unsecure location allowing anyone to access *[Agency Name]* systems and/or FBI CJIS systems and data in your name.
3. Allowing unauthorized person to access FBI CJI at any time for any reason. Note: Unauthorized use of the FBI CJIS systems is prohibited and may be subject to criminal and/or civil penalties.
4. Allowing remote access of *[Agency Name]* issued computer equipment to FBI CJIS systems and/or data without prior authorization by *[Agency Name]*.
5. Obtaining a computer account that you are not authorized to use.
6. Obtaining a password for a computer account of another account owner.
7. Using the *[Agency Name]*'s network to gain unauthorized access to FBI CJI.
8. Knowingly performing an act which will interfere with the normal operation of FBI CJIS systems.
9. Knowingly propagating a computer virus, Trojan horse, worm and malware to circumvent data protection or compromising existing security holes to FBI CJIS systems.
10. Violating terms of software and / or operating system licensing agreements or copyright laws.
11. Duplication of licensed software, except for backup and archival purposes that circumvent copyright laws for use in *[Agency Name]*, for home use or for any customer or contractor.

12. Deliberately wasting computing resources to include streaming audio, videos for personal use that interferes with *[Agency Name]* network performance.
13. Using electronic mail or instant messaging to harass others.
14. Masking the identity of an account or machine.
15. Posting materials publicly that violate existing laws or *[Agency Name]*'s codes of conduct.
16. Attempting to monitor or tamper with another user's electronic mail or files by reading, copying, changing, or deleting without explicit agreement of the owner.
17. Using *[Agency Name]*'s technology resources to advance unwelcome solicitation of a personal or sexual relationship while on duty or through the use of official capacity.
18. Unauthorized possession of, loss of, or damage to *[Agency Name]*'s technology equipment with access to FBI CJI through unreasonable carelessness or maliciousness.
19. Maintaining FBI CJI or duplicate copies of official *[Agency Name]* files in either manual or electronic formats at his or her place of residence or in other physically non-secure locations without express permission.
20. Using *[Agency Name]*'s technology resources and/or FBI CJIS systems for personal or financial gain.
21. Deliberately failing to report promptly any known technology-related misuse by another employee that may result in criminal prosecution or discipline under this policy.
22. Using personally owned devices on *[Agency Name]*'s network to include personally-owned thumb drives, CDs, mobile devices, tablets on wifi, etc. Personally owned devices should not store *[Agency Name]* data, State data, or FBI CJI.

The above listing is not all-inclusive and any suspected technology resource or FBI CJIS system or FBI CJI misuse will be handled by *Agency Name* on a case by case basis. Activities will not be considered misuse when authorized by appropriate *Agency Name* officials for security or performance testing.

Privacy Policy

All agency personnel utilizing agency-issued technology resources funded by *[Agency Name]* expressly acknowledges and agrees that such service, whether for business or personal use, shall remove any expectation of privacy. Use of *[Agency Name]* systems indicates consent to monitoring and recording. The *[Agency Name]* reserves the right to access and audit any and all communications including electronic and physical media at rest, in transit and at end of life. *[Agency Name]* personnel shall not store personal information with an expectation of personal privacy that are under the control and management of *[Agency Name]*.

Personal Use of Agency Technology

The computers, electronic media and services provided by *[Agency Name]* are primarily for business use to assist personnel in the performance of their jobs. Limited, occasional, or incidental use of electronic media (sending or receiving) for personal, non-business purposes is understandable and acceptable, and all such use should be done in a manner that does not negatively affect the systems' use for their business purposes. However, employees are expected to demonstrate a sense of responsibility and not abuse this privilege.

Misuse Notification

Due to the increase in the number of accidental or malicious computer attacks against both government and private agencies, *[Agency Name]* shall: (i) establish an operational incident handling capability for all information systems with access to FBI CJIS systems and data. This includes adequate preparation,

detection, analysis, containment, recovery, and user response activities; (ii) track, document, and report incidents to appropriate agency officials and/or authorities.

ISOs have been identified as the POC on security---related issues for their respective agencies and shall ensure LASOs institute the CSA incident response reporting procedures at the local level.

All *[Agency Name]* personnel are responsible to report misuse of *[Agency Name]* technology resources to appropriate *[Agency Name]* officials.

Local contact---LASO: [firstnamelast@agencyname.com](mailto:firstname.lastname@agencyname.com) Phone:

State contact---CSA ISO: [firstnamelast@state.gov](mailto:firstname.lastname@state.gov) Phone:

I have read the policy and rules above and I will abide in the *[Agency Name]*'s Disciplinary

policy. Signature: _____ Date: _____/20_____

Disposal of Media Policy and Procedures

1.0 Purpose

The purpose of this policy is to outline the proper disposal of media (physical or electronic) at *[Agency Name]*. These rules are in place to protect sensitive and classified information, employees and *[Agency Name]*. Inappropriate disposal of *[Agency Name]* and FBI Criminal Justice Information (CJI) and media may put employees, *[Agency Name]* and the FBI at risk.

2.0 Scope

This policy applies to all *[Agency Name]* employees, contractors, temporary staff, and other workers at *[Agency Name]*, with access to FBI CJIS systems and/or data, sensitive and classified data, and media. This policy applies to all equipment that processes, stores, and/or transmits FBI CJI and classified and sensitive data that is owned or leased by *[Agency Name]*.

3.0 Policy

When no longer usable, hard drives, diskettes, tape cartridges, CDs, ribbons, hard copies, print-outs, and other similar items used to process, store and/or transmit FBI CJI and classified and sensitive data shall be properly disposed of in accordance with measures established by *[Agency Name]*.

Physical media (print-outs and other physical media) shall be disposed of by one of the following methods:

- 1) shredding using *[Agency Name]* issued shredders.
- 2) placed in locked shredding bins for *[private contractor name]* to come on-site and shred, witnessed by *[Agency Name]* personnel throughout the entire process.
- 3) incineration using *[Agency Name]* incinerators or witnessed by *[Agency Name]* personnel onsite at agency or at contractor incineration site, if conducted by non-authorized personnel.

Electronic media (hard-drives, tape cartridge, CDs, printer ribbons, flash drives, printer and copier Hard-drives, etc.) shall be disposed of by one of the <Agency Name> methods:

- 1) **Overwriting (at least 3 times)** - an effective method of clearing data from magnetic media. As the name implies, overwriting uses a program to write (1s, 0s, or a combination of both) onto the location of the media where the file to be sanitized is located.
- 2) **Degaussing** - a method to magnetically erase data from magnetic media. Two types of degaussing exist: strong magnets and electric degausses. Note that common magnets (e.g., those used to hang a picture on a wall) are fairly weak and cannot effectively degauss magnetic media.
- 3) **Destruction** – a method of destroying magnetic media. As the name implies, destruction of magnetic media is to physically dismantle by methods of crushing, disassembling, etc.,

ensuring that the platters have been physically destroyed so that no data can be pulled.

IT systems that have been used to process, store, or transmit FBI CJI and/or sensitive and classified information shall not be released from *[Agency Name]*'s control until the equipment has been sanitized and all stored information has been cleared using one of the above methods.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination.

Information Technology Policy

POLICY 604-01: CYBER SECURITY INCIDENT RESPONSE

An incident, as defined in National Institute of Standards and Technology (NIST) Special Publication 800-61, is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. An incident response capability is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services.

OBJECTIVE:

Ensure theis prepared to respond to cyber security incidents, to protect State systems and data, and prevent disruption of government services by providing the required controls for incident handling, reporting, and monitoring, as well as incident response training, testing, and assistance.

SCOPE:

This policy applies to all Executive Branch agencies, boards, and commissions except those exempt under The Code of

RESPONSIBILITIES:

Individual Information Technology User:

All users of State of_____ computing resources shall be aware of what constitutes a cyber security incident and shall understand incident reporting procedures.

Information Services Division (ISD):

Provide incident response support resources that offer advice and assistance with handling and reporting of security incidents for users of ISD information systems. Incident response support resources may include, for example, the ISD Help Desk, a response team (described below), and access to forensics services.

Establish a Cyber Security Incident Response Team (CSIRT) to ensure appropriate response to cyber security incidents. The CSIRT shall consist of members of the State IT Security Council and key personnel from other agencies as required. CSIRT responsibilities shall be defined in the Cyber Security Incident Reporting Procedures.

Agency Management, Information Technology Organization:

Develop organization and system-level cyber security incident response procedures to ensure management and key personnel are notified of cyber security incidents as required.

Organizations that support information systems shall develop incident response plans and/or procedures that:

- Provides the organization with a roadmap for implementing its incident response capability
- Describes the structure and organization of the incident response capability

- Provides a high-level approach for how the incident response capability fits into the overall organization
- Meets the unique requirements of the organization, which relate to mission, size, structure, and functions
- Defines reportable incidents
- Provides metrics for measuring the incident response capability within the organization
- Defines the resources and management support needed to effectively maintain and mature an incident response capability
- Is reviewed and approved by designated officials within the organization Review incident response plans and procedures at least annually.

Revise the incident response plan/procedures to address system/organizational changes or problems encountered during implementation, execution, or testing.

Distribute copies of the incident response plan/procedures to incident response personnel.

Communicate incident response plan/procedure changes to incident response personnel and other organizational elements as needed.

Provide incident response training to information system users consistent with assigned roles and responsibilities before authorizing access to the information system or performing assigned duties, when required by information system changes; and annually thereafter.

Organizations shall test the incident response capability for the information systems they support at least annually. Use organization-defined tests and/or exercises to determine incident response effectiveness. Document the results.

Organizations that support information systems shall implement an incident handling capability for cyber security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

Coordinate incident handling activities with contingency planning activities.

Incorporate the lessons learned from prior and ongoing incident handling activities into incident response procedures, training, and testing/exercises.

Track and document information system security incidents. Retain and safeguard cyber security incident documentation as evidence for investigation, corrective actions, potential disciplinary actions, and/or prosecution.

Promptly report cyber security incident information to appropriate authorities in accordance with State or organization incident reporting procedures.

Organizations that support information systems shall provide an incident response support resource integral to the organizational incident response capability that offers advice and assistance to users of the information

system for the handling and reporting of security incidents.

Possible implementations of incident response support resources in an organization include a help desk or an assistance group and, when required, access to forensics services.

ADDITIONAL INFORMATION:

Information Technology Procedure 604P1: Cyber Security Incident Reporting

[http://cybersecurity.alabama.gov/documents/Procedure 604P1 Incident Reporting.pdf](http://cybersecurity.alabama.gov/documents/Procedure_604P1_Incident_Reporting.pdf)

Information Technology Procedure 604P2: Cyber Security Incident Handling

[http://cybersecurity.alabama.gov/documents/Procedure 604P2 Incident Handling.pdf](http://cybersecurity.alabama.gov/documents/Procedure_604P2_Incident_Handling.pdf)

Information Technology Dictionary [http://cybersecurity.alabama.gov/documents/IT Dictionary.pdf](http://cybersecurity.alabama.gov/documents/IT_Dictionary.pdf)

By Authority of Director, Information Services Division, Department of Finance

DOCUMENT HISTORY:

Version	Release Date	Comments
604-00	06/16/2011	Combines and replaces Policy 600-04 and Standard 600-04S1
604-01	07/19/2012	Reorganized requirements under Agency Responsibilities, and updated consistent with NIST 800-53 and 800-61 guidance

Policy Title:	Media Protection Policy
Effective Date:	
Revision Date:	Every 2 years or as needed
Approval(s):	
LASO:	
CSO:	
Agency Head:	

Purpose:

The intent of the Media Protection Policy is to ensure the protection of the Criminal Justice Information (CJI) until such time as the information is either released to the public via authorized dissemination (e.g. within a court system or when presented in crime reports data), or is purged or destroyed in accordance with applicable record retention rules.

This Media Protection Policy was developed using the FBI’s Criminal Justice Information Services (CJIS) Security Policy 5.1 dated 7/13/2012. The *[agency name]* may complement this policy with a local policy; however, the CJIS Security Policy shall always be the minimum standard. The local policy may augment, or increase the standards, but shall not detract from the CJIS Security Policy standards.

Scope:

The scope of this policy applies to any electronic or physical media containing FBI Criminal Justice Information (CJI) while being stored, accessed or physically moved from a secure location from the *[agency name]*. This policy applies to any authorized person who accesses, stores, and / or transports electronic or physical media. Transporting CJI outside the agency’s assigned physically secure area must be monitored and controlled.

Authorized *[agency name]* personnel shall protect and control electronic and physical CJI while at rest and in transit. The *[agency name]* will take appropriate safeguards for protecting CJI to limit potential mishandling or loss while being stored, accessed, or transported. Any inadvertent or inappropriate CJI disclosure and/or use will be reported to the *[agency name]* Local Agency Security Officer (LASO). Procedures shall be defined for securely handling, transporting and storing media.

Media Storage and Access:

Controls shall be in place to protect electronic and physical media containing CJI while at rest, stored, or actively being accessed. “Electronic media” includes memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card. “Physical media” includes printed documents and imagery that contain CJI.

To protect CJI, the *[agency name]* personnel shall:

1. Securely store electronic and physical media within a physically secure or controlled area. A secured area includes a locked drawer, cabinet, or room.
2. Restrict access to electronic and physical media to authorized individuals.
3. Ensure that only authorized users remove printed form or digital media from the CJI.
4. Physically protect CJI until media end of life. End of life CJI is destroyed or sanitized using approved equipment, techniques and procedures. (See Sanitization Destruction Policy)
5. Not use personally owned information system to access, process, store, or transmit CJI unless the *[agency name]* has established and documented the specific terms and conditions for personally owned information system usage. (See Personally Owned Device Policy)
6. Not utilize publicly accessible computers to access, process, store, or transmit CJI. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.
7. Store all hardcopy CJI printouts maintained by the *[agency name]* in a secure area accessible to only those employees whose job function require them to handle such documents.
8. Safeguard all CJI by the *[agency name]* against possible misuse by complying with the Physical Protection Policy, Personally Owned Device Policy, and Disciplinary Policy.
9. Take appropriate action when in possession of CJI while not in a secure area:
 - a. CJI must not leave the employee's immediate control. CJI printouts cannot be left unsupervised while physical controls are not in place.
 - b. Precautions must be taken to obscure CJI from public view, such as by means of an opaque file folder or envelope for hard copy printouts. For electronic devices like laptops, use session lock use and /or privacy screens. CJI shall not be left in plain public view. When CJI is electronically transmitted outside the boundary of the physically secure location, the data shall be immediately protected using encryption.
 - i. When CJI is at rest (i.e. stored electronically) outside the boundary of the physically secure location, the data shall be protected using encryption. Storage devices include external hard drives from computers, printers and copiers used with CJI. In addition, storage devices include thumb drives, flash drives, back---up tapes, mobile devices, laptops, etc.
 - ii. When encryption is employed, the cryptographic module used shall be certified to meet FIPS 140---2 standards.
10. Lock or log off computer when not in immediate vicinity of work area to protect CJI. Not all personnel have same CJI access permissions and need to keep CJI protected on a need---to---know basis.

11. Establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of CJI. (See Physical Protection Policy)

Media Transport:

Controls shall be in place to protect electronic and physical media containing CJI while in transport (physically moved from one location to another) to prevent inadvertent or inappropriate disclosure and use. "Electronic media" means electronic storage media including memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card.

Dissemination to another agency is authorized if:

1. The other agency is an Authorized Recipient of such information and is being serviced by the accessing agency, or
2. The other agency is performing personnel and appointment functions for criminal justice employment applicants.

The *[agency name]* personnel shall:

1. Protect and control electronic and physical media during transport outside of controlled areas.
2. Restrict the pickup, receipt, transfer and delivery of such media to authorized personnel.

The *[agency name]* personnel will control, protect, and secure electronic and physical media during transport from public disclosure by:

1. Use of privacy statements in electronic and paper documents.
2. Limiting the collection, disclosure, sharing and use of CJI.
3. Following the least privilege and role based rules for allowing access.
Limit access to CJI to only those people or roles that require access.
4. Securing hand carried confidential electronic and paper documents by:
 - a. Storing CJI in a locked briefcase or lockbox.
 - b. Only viewing or accessing the CJI electronically or document printouts in a physically secure location by authorized personnel.
 - c. For hard copy printouts or CJI documents:
 - i. Package hard copy printouts in such a way as to not have any CJI information viewable.
 - ii. That are mailed or shipped, agency must document procedures and only release to authorized individuals. **DO NOT MARK THE PACKAGE TO BE MAILED CONFIDENTIAL.** Packages containing CJI material are to be sent by method(s) that provide for complete shipment tracking and history, and signature confirmation of delivery. (Agency Discretion)
5. Not taking CJI home or when traveling unless authorized by *[agency name]* LASO. When disposing confidential documents, use a shredder.

Electronic Media Sanitization and Disposal:

The agency shall sanitize, that is, overwrite at least three times or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. Inoperable electronic media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel. Physical media shall be securely disposed of when no longer required, using formal procedures. For end of life media policy, refer to “Sanitization Destruction Policy”.

Breach Notification and Incident Reporting:

The agency shall promptly report incident information to appropriate authorities. Information security events and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken. Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

Roles and Responsibilities:

If CJI is improperly disclosed, lost, or reported as not received, the following procedures must be immediately followed:

1. *[agency name]* personnel shall notify his/her supervisor or LASO, and an incident---report form must be completed and submitted within 24 hours of discovery of the incident. The submitted report is to contain a detailed account of the incident, events leading to the incident, and steps taken/to be taken in response to the incident. (Agency Discretion)
2. The supervisor will communicate the situation to the LASO to notify of the loss or disclosure of CJI records.
3. The LASO will ensure the CSA ISO (CJIS System Agency Information Security Officer) is promptly informed of security incidents.
4. The CSA ISO will:
 - a. Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CSA, the affected criminal justice agency, and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI.
 - b. Collect and disseminate all incident---related information received from the Department of Justice (DOJ), FBI CJIS Division, and other entities to the appropriate local law enforcement POCs within their area.
 - c. Act as a single POC for their jurisdictional area for requesting incident response assistance.

Penalties:

Violation of any of the requirements in this policy by any authorized personnel will result in suitable disciplinary action, up to and including loss of access privileges, civil and criminal prosecution and / or termination.

Acknowledgement:

I have read the policy and rules above and I will:

- Abide by the *[agency name]*'s Media Protection Policy. I understand any violation of this policy may result in discipline up to and including termination.
- Report any *[agency name]* CJI security incident to Supervisor and / or LASO as identified in this policy.

Signature: _____ Date: _____/2012_____

Questions

Any questions related to this policy may be directed to the *[agency name]*'s LASO:

LASO Name:	LASO Phone:	LASO email:
State C/ISO Name:	C/ISO Phone:	C/ISO email:

Policy Title:	Allowed Personally Owned Device Policy
Effective Date:	
Revision Date:	Every 2 years or as needed
Approval(s):	
LASO:	
CSO:	
Agency Head:	

Purpose:

A personally owned information system or device shall be authorized to access, process, store or transmit [agency name], state, or FBI Criminal Justice Information (CJI) only when these established and documented specific terms and conditions are met. This control does not apply to the use of personally owned information systems to access the [agency name]'s information systems and information that are intended for public access (e.g., an agency's public website that contains purely public information).

This Personally Owned Device Policy was developed using the FBI's *CJIS Security Policy* 5.1 dated July 13, 2012. The intended target audience is [agency name] personnel, support personnel and private contractors/vendors. The [agency name] may complement this policy with a local policy; however, the *CJIS Security Policy* shall always be the minimum standard and the local policy may augment, or increase the standards, but shall not detract from the *CJIS Security Policy* standards.

Scope:

This policy applies to all [agency name] personnel, support personnel, and/or private contractors/vendors who are authorized to use personally owned devices to connect to any physical, logical, and/or electronic premise of the [agency name] to access, process, store, and/or transmit CJI. This also includes any private contractors/vendors who will conduct maintenance on any network device that processes, stores, and/or transmits FBI CJI.

Personally Owned Devices:

A personally owned device is any technology device that was purchased by an individual and was not issued by the [agency name]. A personal device includes any portable technology like camera, USB flash drives, USB thumb drives, DVDs, CDs, air cards and mobile wireless devices such as Androids, Blackberry OS, Apple iOS, Windows Mobile, Symbian, tablets, laptops or any personal desktop computer. Threats to mobile handheld devices stem mainly from their size, portability, and available wireless interfaces and associated services.

The [agency name] will maintain management control and authorize the use of personally owned devices. The [agency name] shall develop guidelines to define which employees can use their own devices, the types of devices they can use, and which applications and data they can access, process, or store on their devices.

Personally owned devices must:

- Be authorized by [agency name] to access, process, transmit, and/or store FBI CJI.
- Be inspected by [agency name]'s IT staff and the LASO to ensure appropriate security requirements on the device are up-to-date and meet the FBI's *CJIS Security Policy* requirements prior to use.
- Take necessary precautions when using device outside of a physically secure area. Read below and also see Physical Protection Policy.

Remote Access:

The [agency name] shall authorize, monitor, and control all methods of remote access to the information systems that can access, process, transmit, and/or store FBI CJI. Remote access is any temporary access to an agency's information system by a user (or an information system) communicating temporarily through an external, non-agency controlled network (e.g., the Internet).

The [agency name] shall employ automated mechanisms to facilitate the monitoring and control of remote access methods. The [agency name] shall control all remote accesses through managed access control points. The [agency name] may permit remote access for privileged functions only for compelling operational needs but shall document the rationale for such access in the security plan for the information system.

Utilizing publicly accessible computers to access, process, store or transmit CJI is prohibited. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

Roles and Responsibilities:

Owner Role: The owner agrees to:

1. Follow necessary policy and procedures to protect FBI CJI.
2. Usage of their device will be for work-related purposes.
3. Bring their device to work to use during normal work hours and not share the device with anyone else.
4. [agency name] having the authority to erase device remotely as needed.
5. Be responsible for any financial obligations for device.
6. Protect individual's and [agency name]'s privacy.
7. Use good judgement before installing free applications. Sometimes free applications track your personal information with limited disclosure or authorization, and then sell your profile to advertising companies.
8. Use good judgement on amount of time applied to personal use of personally owned devices during normal work business hours.
9. Access FBI CJI only from an approved and authorized storage device.
10. Do not stream music or videos using personally owned devices when connected to [agency name]'s network to prevent sluggishness.

11. Report lost or stolen mobile or storage devices to the [agency name]'s Local Agency Security Officer (LASO) within one business day.
12. Review the use of device alerts and update services to validate you requested them. Restrict notifications not requested by looking at your device's settings.
13. Control wireless network and service connectivity. Validate mobile device default settings are not connecting to nearby Wi-Fi networks automatically. Some of these networks, like in airports or neighborhood coffee shops, may be completely open and unsecure.

Information Technology Role

The [agency name] IT support role shall, at a minimum, ensure that external storage devices:

1. Are encrypted when FBI CJI is stored electronically.
2. Are scanned for virus and malware prior to use and/or prior to being connected to the agency's computer or laptop.

The [agency name] IT support role shall, at a minimum, ensure that all personally owned devices:

1. Apply available critical patches and upgrades to the device operating system.
2. Are kept updated with security patches, firmware updates and antivirus.
3. Are configured for local device authentication.
4. Use advanced authentication and encryption when FBI CJI is stored and/or transmitted.
5. Be able to deliver built-in identity role-mapping, network access control (NAC), AAA (Authentication, Authorization, and Accounting) services, and real-time endpoint reporting.
6. Erase cached information when session is terminated.
7. Employ personal firewalls.
8. Minimize security risks by ensuring antivirus and antimalware are installed, running real time and updated.
9. Be scanned for viruses and malware prior to accessing or connecting to [agency name] CJIS network.
10. Configure Bluetooth interface as undiscoverable except as needed for pairing, which prevents visibility to other Bluetooth devices except when discovery is specifically needed.
11. Be properly disposed of at end of life. See Media Disposal Policy. Remove FBI CJI before owner sells their personally owned devices or sends it in for repairs.
12. Evaluate personally owned device age. Older device hardware is too outdated for needed updates. Typical life is two years.
13. Ensure device is compatible with needed network protocols and/or compatible with customized applications developed for access FBI CJI through testing.
14. Deploy Mobile Device Management or SIM card locks and credential functions. The credential functions require a pass code to use [agency name]'s network services. *(Research enterprise mobile device management solutions-- see product working successfully in real life scenario with the type of mobile device your*

State/Agency wants to use prior to implementing. The enterprise mobile device solution must be compatible with chosen device products.)

15. Ensure owner and IT staff have mobile backup enabled to an approved [agency name] location. Set a daily or weekly schedule to periodically synch data and applications. If backup contains FBI CJI, take appropriate security measures for storage of FBI CJI. See Media Protection Policy.
16. Retain the ability to secure, control and remotely erase agency data on employee---owned devices in the event of a security breach or if the employee leaves the agency employment or the device is lost or stolen. This remote ability can be done through technology that allows virtual access to company applications.
17. Enable mobile device in a “find my phone” service to allow finding device.
18. Consider adding extra protection such as a total device reset if the PIN is guessed incorrectly a certain number of attempts.
19. Be able to easily identify connected users and devices. Track, log and manage every personally used device allowed to connect to agency technology resources for secure FBI CJI access.
20. Perform pre and post---authentication checks.
21. Ability to allow and deny access. Selectively grant proper network access privileges.

Local Area Security Officer (LASO)

The LASO will:

1. Identify who is using the personally owned approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
2. Identify and document how the equipment is connected to the state system.
3. Ensure that personnel security screening procedures are being followed as stated in this policy.
4. Ensure the approved and appropriate security measures are in place and working as expected.
5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

Penalties:

Violation of any of the requirements in this policy by any authorized personnel will result in suitable disciplinary action, up to and including loss of access privileges, civil and criminal prosecution and/or termination. Personally owned information technology resources used may be retained by the [agency name] for evaluation in investigation of security violations.

Violation of any of the requirements in this policy by any unauthorized person can result in similar disciplinary action against the device owner, and can also result in termination of services with any associated consulting organization or prosecution in the case of criminal activity.

Acknowledgement:

The [agency name], agency personnel, IT support, private contractors/vendors, and the LASO alike will agree to commit to all bring your own (BYO) rules.

I have read the policy and rules above and I will:

- Authorize the [agency name] to remotely wipe my mobile device.
- Abide by the [agency name] Personally Owned Device policy. I understand any violation of this policy may result in discipline up to and including termination.
- Complete the security awareness training and take action to protect [agency name] facilities, personnel and associated information systems.
- Report any unauthorized device access to [agency name] LASO.

Signature: _____ Date: _____/20_____

Questions

Any questions related to this policy may be directed to the [agency name]'s LASO:

LASO Name:	LASO Phone:	LASO email:
State CSO/ISO Name:	CSO/ISO Phone:	CSO/ISO email:

Other Related Policy Reference:

- See Media Sanitization and Destruction Policy
- Physical Protection Policy

Policy Title:	Physical Protection Policy
Effective Date:	
Revision Date:	Every 2 years or as needed
Subject Matter Experts / Approval(s):	
TAC:	
LASO:	
C/ISO:	
Front Desk:	
Technology Support Lead:	
Agency Head:	

Purpose:

The purpose of this policy is to provide guidance for agency personnel, support personnel, and private contractors/vendors for the physical, logical, and electronic protection of Criminal Justice Information (CJI). All physical, logical, and electronic access must be properly documented, authorized and controlled on devices that store, process, or transmit unencrypted CJI. This Physical Protection Policy focuses on the appropriate access control methods needed to protect the full lifecycle of CJI from insider and outsider threats.

This Physical Protection Policy was developed using the FBI’s *CJIS Security Policy 5.1* dated July 13, 2012. The intended target audience is [agency name] personnel, support personnel, and private contractor/vendors with access to CJI whether logically or physically. The local agency may complement this policy with a local policy; however, the *CJIS Security Policy* shall always be the minimum standard and local policy may augment, or increase the standards, but shall not detract from the *CJIS Security Policy* standards.

Physically Secure Location:

A physically secure location is a facility or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect the FBI CJI and associated information systems. The perimeter of the physically secure location shall be prominently posted and separated from non---secure locations by physical controls. Security perimeters shall be defined, controlled, and secured. Restricted non---public areas in the [agency name] shall be identified with a sign at the entrance.

Visitors Access:

A visitor is defined as a person who visits the [agency name] facility on a temporary basis who is not employed by the [agency name] and has no unescorted access to the physically secure location within the [agency name] where FBI CJI and associated information systems are located. For agencies with jails with CJIS terminals, additional visit specifications need to be established per agency purview and approval.

Visitors shall:

1. Check in before entering a physically secure location by:
 - a. Completing the visitor access log, which includes: name and visitor's agency, purpose for the visit, date of visit, time of arrival and departure, name and agency of person visited, and form of identification used to authenticate visitor.
 - b. Document badge number on visitor log if visitor badge issued. If [agency name] issues visitor badges, the visitor badge shall be worn on approved visitor's outer clothing and collected by the agency at the end of the visit.
 - c. Planning to check or sign-in multiple times if visiting multiple physically secured locations and/or building facilities that are not adjacent or bordering each other that each has their own individual perimeter security to protect CJI.
2. Be accompanied by a [agency name] escort at all times to include delivery or service personnel. An escort is defined as an authorized personnel who accompanies a visitor at all times while within a physically secure location to ensure the protection and integrity of the physically secure location and any CJI therein. The use of cameras or other electronic means used to monitor a physically secure location does not constitute an escort.
3. Show [agency name] personnel a valid form of photo identification.
4. Follow [agency name] policy for authorized unescorted access.
 - a. Noncriminal Justice Agency (NCJA) like city or county IT who require frequent unescorted access to restricted area(s) will be required to establish a Management Control Agreement between the [agency name] and NCJA. Each NCJA employee with CJI access will appropriately have state and national fingerprint--based record background check prior to this restricted area access being granted.
 - b. Private contractors/vendors who requires frequent unescorted access to restricted area(s) will be required to establish a Security Addendum between the [agency name] and each private contractor personnel. Each private contractor personnel will appropriately have state and national fingerprint---based record background check prior to this restricted area access being granted.
5. Not be allowed to view screen information mitigating shoulder surfing.
6. Individuals not having any legitimate business in a restricted area shall be courteously escorted to a public area of the facility. Strangers in physically secure areas without an escort should be challenged. If resistance or behavior of a threatening or suspicious nature is encountered, sworn personnel shall be notified or call 911.
7. Not be allowed to sponsor another visitor.
8. Not enter into a secure area with electronic devices unless approved by the [agency name] Local Area Security Officer (LASO) to include cameras and mobile devices. Photographs are not allowed without permission of the [agency name] assigned personnel.
9. All requests by groups for tours of the [agency name] facility will be referred to the proper agency point of contact for scheduling. In most cases, these groups will be handled by a single form, to be signed by a designated group leader or representative. Remaining visitor rules apply for each visitor within the group. The group leader will provide a list of names to front desk personnel for instances of emergency evacuation and accountability of each visitor while on agency premises.

Authorized Physical Access:

Only authorized personnel will have access to physically secure non---public locations. The [agency name] will maintain and keep current a list of authorized personnel. All physical access points into the agency's secure areas will be authorized before granting access. The agency will implement access controls and monitoring of physically secure areas for protecting all transmission and display mediums of CJI. Authorized personnel will take necessary steps to prevent and protect the agency from physical, logical and electronic breaches.

All personnel with CJI physical and logical access must:

1. Meet the minimum personnel screening requirements prior to CJI access.
 - a. To verify identification, a state of residency and national fingerprint---based record checks shall be conducted within 30 days of assignment for all personnel who have direct access to CJI and those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI.
 - b. Support personnel, private contractors/vendors, and custodial workers with access to physically secure locations or controlled areas (during CJI processing) shall be subject to a state and national fingerprint---based record check unless these individuals are escorted by authorized personnel at all times.
 - c. Prior to granting access to CJI, the [agency name] on whose behalf the contractor is retained shall verify identification via a state of residency and national fingerprint---based record check.
 - d. Refer to the *CJIS Security Policy* for handling cases of felony convictions, criminal records, arrest histories, etc.
2. Complete security awareness training.
 - a. All authorized [agency name], Noncriminal Justice Agencies (NCJA) like city or county IT and private contractor/vendor personnel will receive security awareness training within six months of being granted duties that require CJI access and every two years thereafter.
 - b. Security awareness training will cover areas specified in the *CJIS Security Policy* at a minimum.
3. Be aware of who is in their secure area before accessing confidential data.
 - a. Take appropriate action to protect all confidential data.
 - b. Protect all terminal monitors with viewable CJI displayed on monitor and not allow viewing by the public or escorted visitors.
4. Properly protect and not share any individually issued keys, proximity cards, computer account passwords, etc.
 - a. Report loss of issued keys, proximity cards, etc to authorized agency personnel.
 - b. If the loss occurs after normal business hours, or on weekends or holidays, personnel are to call the [agency name] POC to have authorized credentials like a proximity card de---activated and/or door locks possibly rekeyed.
 - c. Safeguard and not share passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), and all other facility and computer systems security access procedures. See Disciplinary Policy.
5. Properly protect from viruses, worms, Trojan horses, and other malicious code.

6. Web usage—allowed versus prohibited; monitoring of user activity. (allowed versus prohibited is at the agency’s discretion)
7. Do not use personally owned devices on the [agency name] computers with CJI access. (Agency discretion). See Personally Owned Policy.
8. Use of electronic media is allowed only by authorized [agency name] personnel. Controls shall be in place to protect electronic media and printouts containing CJI while in transport. When CJI is physically moved from a secure location to a non---secure location, appropriate controls will prevent data compromise and/or unauthorized access.
9. Encrypt emails when electronic mail is allowed to transmit CJI---related data as such in the case of Information Exchange Agreements.
 - a. (Agency Discretion for allowance of CJI via email)
 - b. If CJI is transmitted by email, the email must be encrypted and email recipient must be authorized to receive and view CJI.
10. Report any physical security incidents to the [agency name]’sLASO to include facility access violations, loss of CJI, loss of laptops, Blackberries, thumb drives, CDs/DVDs and printouts containing CJI.
11. Properly release hard copy printouts of CJI only to authorized vetted and authorized personnel in a secure envelope and shred or burn hard copy printouts when no longer needed. Information should be shared on a “need to know” basis. (See Sanitization and Destruction Policy)
12. Ensure data centers with CJI are physically and logically secure.
13. Keep appropriate [agency name] security personnel informed when CJI access is no longer needed. In the event of ended employment, the individual must surrender all property and access managed by the local agency, state and/or federal agencies.
14. Not use food or drink around information technology equipment.
15. Know which door to use for proper entry and exit of the [agency name] and only use marked alarmed fire exits in emergency situations.
16. Ensure the perimeter security door securely locks after entry or departure. Do not leave any perimeter door propped opened and take measures to prevent piggybacking entries.

Roles and Responsibilities:

Terminal Agency Coordinator (TAC)

The TAC serves as the point---of---contact at the [agency name] for matters relating to CJIS information access. The TAC administers CJIS systems programs within the agency and oversees the agency’s compliance with FBI and state CJIS systems policies.

Local Agency Security Officer (LASO)

Each LASO shall:

1. Identify who is using the CSA (state) approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
2. Identify and document how the equipment is connected to the state system.
3. Ensure that personnel security screening procedures are being followed as stated in this policy.
4. Ensure the approved and appropriate security measures are in place and working as expected.
5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

Agency Coordinator (AC)

An AC is a staff member of the Contracting Government Agency (CGA) who manages the agreement between the private contractor(s)/vendor(s) and the [agency name]. A CGA is a government agency, whether a Criminal Justice Agency (CJA) or a NCJA, that enters into an agreement with a private contractor/vendor subject to the CJIS Security Addendum. The AC shall be responsible for the supervision and integrity of the system, training and continuing education of private contractor/vendor employees and operators, scheduling of initial training and testing, and certification testing and all required reports by NCIC.

CJIS System Agency Information Security Officer (CSA ISO)

The CSA ISO shall:

1. Serve as the security point of contact (POC) to the FBI CJIS Division ISO.
2. Document technical compliance with the CJIS Security Policy with the goal to assure the confidentiality, integrity, and availability of criminal justice information to the user community throughout the CSA's user community, to include the local level.
3. Document and provide assistance for implementing the security---related controls for the Interface Agency and its users.
4. ISOs have been identified as the POC on security---related issues for their respective agencies and shall ensure LASOs institute the CSA incident response reporting procedures at the local level. Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CSA, the affected criminal justice agency, and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI.

Information Technology Support

In coordination with above roles, all vetted IT support staff will protect CJI from compromise at the [agency name] by performing the following:

1. Protect information subject to confidentiality concerns—in systems, archived, on backup media, and until destroyed. Know where CJI is stored, printed, copied, transmitted and planned end of life. CJI is stored on laptops, mobile data terminals (MDTs), computers, servers, tape backups, CDs, DVDs, thumb drives, RISC devices and internet connections as authorized by the [agency name]. For agencies who submit fingerprints using Live Scan terminals, only Live Scan terminals that receive CJI back to the Live Scan terminal will be assessed for physical security.
2. Be knowledgeable of required [agency name] technical requirements and policies taking appropriate preventative measures and corrective actions to protect CJI at rest, in transit and at the end of life.
3. Take appropriate action to ensure maximum uptime of CJI and expedited backup restores by using agency approved best practices for power backup and data backup means such as generators, backup universal power supplies on CJI---based terminals, servers, switches, etc.
4. Properly protect the [agency name]'s CJIS system(s) from viruses, worms, Trojan horses, and other malicious code (real---time scanning and ensure updated definitions).
 - a. Install and update antivirus on computers, laptops, MDTs, servers, etc.

- b. Scan any outside non---agency owned CDs, DVDs, thumb drives, etc., for viruses, if the [agency name] allows the use of personally owned devices. (See the [agency name] Personally Owned Device Policy)
- 5. Data backup and storage—centralized or decentralized approach.
 - a. Perform data backups and take appropriate measures to protect all stored CJI.
 - b. Ensure only authorized vetted personnel transport off---site tape backups or any other media that store CJI that is removed from physically secured location.
 - c. Ensure any media released from the [agency name] is properly sanitized / destroyed. (See Sanitization and Destruction Policy)
- 6. Timely application of system patches—part of configuration management.
 - a. The agency shall identify applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws.
 - b. When applicable, see the [agency name] Patch Management Policy.
- 7. Access control measures
 - a. Address least privilege and separation of duties.
 - b. Enable event logging of:
 - i. Successful and unsuccessful system log---on attempts.
 - ii. Successful and unsuccessful attempts to access, create, write, delete or change permission on a user account, file, directory or other system resource.
 - iii. Successful and unsuccessful attempts to change account passwords.
 - iv. Successful and unsuccessful actions by privileged accounts.
 - v. Successful and unsuccessful attempts for users to access, modify, or destroy the audit log file.
 - c. Prevent authorized users from utilizing publicly accessible computers to access, process, store, or transmit CJI. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.
- 8. Account Management in coordination with TAC
 - a. Agencies shall ensure that all user IDs belong to currently authorized users.
 - b. Keep login access current, updated and monitored. Remove or disable terminated or transferred or associated accounts.
 - c. Authenticate verified users as uniquely identified.
 - d. Prevent multiple concurrent active sessions for one user identification, for those applications accessing CJI, unless the agency grants authority based upon operational business needs.
 - e. Not use shared generic or default administrative user accounts or passwords for any device used with CJI.
 - f. Passwords
 - i. Be a minimum length of eight (8) characters on all systems.
 - ii. Not be a dictionary word or proper name.
 - iii. Not be the same as the Userid.
 - iv. Expire within a maximum of 90 calendar days.

- v. Not be identical to the previous ten (10) passwords.
 - vi. Not be transmitted in the clear or plaintext outside the secure location.
 - vii. Not be displayed when entered.
 - viii. Ensure passwords are only reset for authorized user.
9. Network infrastructure protection measures.
- a. Take action to protect CJI---related data from unauthorized public access.
 - b. Control access, monitor, enabling and updating configurations of boundary protection firewalls.
 - c. Enable and update personal firewall on mobile devices as needed.
 - d. Ensure confidential electronic data is only transmitted on secure network channels using encryption and *advanced authentication when leaving a physically secure location. No confidential data should be transmitted in clear text. **Note: for interim compliance, and for the sole purpose of meeting the advanced authentication policy, a police vehicle shall be considered a physically secure location until September 30th 2013. For the purposes of this policy, a police vehicle is defined as an enclosed criminal justice conveyance with the capability to comply, during operational periods.*
 - e. Ensure any media that is removed from a physically secured location is encrypted in transit by a person or network.
 - f. Not use default accounts on network equipment that passes CJI like switches, routers, firewalls.
 - g. Make sure law enforcement networks with CJI shall be on their own network accessible by authorized personnel who have been vetted by the [agency name]. Utilize Virtual Local Area Network (VLAN) technology to segment CJI traffic from other noncriminal justice agency traffic to include other city and/or county agencies using same wide area network.
10. Communicate and keep the [agency name] informed of all scheduled and unscheduled network and computer downtimes, all security incidents and misuse. The ultimate information technology management control belongs to [agency name].

Front desk and Visitor Sponsoring Personnel

Administration of the Visitor Check---In / Check---Out procedure is the responsibility of identified individuals in each facility. In most facilities, this duty is done by the Front desk or Reception Desk.

Prior to visitor gaining access to physically secure area:

1. The visitor will be screened by the [agency name] personnel for weapons. No weapons are allowed in the agency except when carried by authorized personnel as deemed authorized by the [agency name].
2. The visitor will be screened for electronic devices. No personal electronic devices are allowed in any agency facility except when carried by authorized personnel as deemed authorized by the [agency name].
3. Escort personnel will acknowledge being responsible for properly evacuating visitor in cases of emergency. Escort personnel will know appropriate evacuation

routes and procedures.

4. Escort and/or Front desk personnel will validate visitor is not leaving agency with any agency owned equipment or sensitive data prior to Visitor departure.

All [agency name] personnel and supporting entities are responsible to report any unauthorized physical, logical, and electronic access to the [agency name] officials. For [agency name], the point of contacts to report any non---secure access is:

LASO Name:	LASO Phone:	LASO email:
AC Name:	AC Phone:	AC email:
State C/ISO Name:	C/ISO Phone:	C/ISO email:

Penalties:

Violation of any of the requirements in this policy by any authorized personnel will result in suitable disciplinary action, up to and including loss of access privileges, civil and criminal prosecution and / or termination.

Violation of any of the requirements in this policy by any visitor can result in similar disciplinary action against the sponsoring employee, and can also result in termination of services with any associated consulting organization or prosecution in the case of criminal activity.

Acknowledgement:

I have read the policy and rules above and I will:

- Abide by the [agency name] Physical Protection Policy. I understand any violation of this policy may result in discipline up to and including termination.
- Complete the security awareness training and take action to protect the [agency name]'s facilities, personnel and associated information systems.
- Report any unauthorized physical access to the [agency name]'s LASO.

Signature: _____ Date: _____/2012_

Other Related Policy Reference:

- Sanitization and Destruction Policy
- Disciplinary Policy
- *CJIS Security Policy*

User Rules of Behavior Acknowledgment Form

As a user of an IT system, I acknowledge my responsibility to conform to the following requirements and conditions as directed by all relevant Information Assurance and Information Security Policies, Procedures and Guidelines. These conditions apply to all personnel who have access to FBI CJIS systems and all appropriate IT personnel.

1. I understand that failure to sign this acknowledgment will result in denial of access to FBI CJIS systems, terminal areas, and facilities that have FBI CJIS network equipment.
2. I acknowledge my responsibility to use the network only for official business except for such personal use involving negligible cost to the agency and no interference with official business as may be permissible under the acceptable use policy.
3. I understand that the network operates at a Sensitive but Unclassified level. I have all clearance necessary for access to the network, and will not introduce or process data that the network is not specifically designed to handle as specified by the Security Policy.
4. I understand the need to protect my password at the highest level of data it secures. I will NOT share my password and/or account. I understand that neither the Security Administrator/System Administrator, nor the Network Operations Center (NOC) will request my password. I will change my password at least every 90 days or as requested for security reasons.
5. I understand I am responsible for all actions taken under my account. I will not attempt to “hack” the network or any connected automated information system (AIS), or attempt to gain access to data for which I am not specifically authorized.
6. I understand my responsibility to appropriately protect all output generated under my account, to include printed material, magnetic tapes, floppy disks, CD-ROMs, and downloaded hard disk files. I understand that I am required to ensure all hard copy material and magnetic media is properly labeled as required by policies and regulations.
7. I understand my responsibility to report all AIS or network problems to my security point of contact. I will NOT install, remove, or modify any hardware or software.
8. I acknowledge my responsibility to not introduce any software or hardware not acquired and approved through the IT Security group. I also acknowledge my

responsibility to have all official electronic media virus-scanned by the IT Security group before introducing it into the AIS or network.

9. I acknowledge my responsibility to conform to the requirements of the Rules of Behavior, Acceptable Use Policy, and Security Policies and Procedures. I also acknowledge that failure to comply with these policies and procedures may constitute a security violation resulting in denial of access to the AIS, network, or facilities, and that such violations will be reported to appropriate authorities for further actions as deemed appropriate to include disciplinary, civil, or criminal penalties.
10. I agree that I have no expectation of privacy in any equipment or media I use. I consent to inspections by authorized agency personnel, at any time and agree to make any equipment available for audit and review by FBI personnel upon request.
11. I further consent that my use of FBI CJIS systems within agency owned or leased space is subject to system monitoring.
12. I have completed the required triennial Security Awareness Training required by the *CJIS Security Policy* for individuals managing or accessing FBI CJIS systems and/or data.

User (Print Name): _____ **Date:** _____

User Signature: _____ **Date:** _____

ISO/Security Officer: _____ **Date:** _____

Policy Title:	User Account / Access Validation Policy
Effective Date:	
Revision Date:	Every 2 years or as needed
Subject Matter Experts / Approval(s):	
TAC:	
LASO:	
C/ISO:	
Front Desk:	
Technology Support Lead:	
Agency Head:	

Purpose:

All accounts shall be reviewed at least every six months by the terminal agency coordinator (TAC) or his/her designee to ensure that access and account privileges commensurate with job functions, need-to-know, and employment status on systems that contain Criminal Justice Information. The TAC may also conduct periodic reviews.

All guest accounts (for those who are not official employees of the CJA) with access to the criminal justice network shall contain an expiration date of one year or the work completion date, whichever occurs first. All guest accounts (for private contractor personnel) must be sponsored by the appropriate authorized member of the administrative entity managing the resource.

The TAC must disable all new accounts that have not been accessed within 30 days of creation. Accounts of individuals on extended leave (more than 30 days) should be disabled. (Note: Exceptions can be made in cases where uninterrupted access to IT resources is required. In those instances, the individual going on extended leave must have a manager-approved request from the designated account administrator or assistant.)

The TAC must be notified if a user's information system usage or need-to-know changes (i.e., the employee is terminated, transferred, etc.). If an individual is assigned to another office for an extended period (more than 90 days), the TAC will transfer the individual's account(s) to the new office (CJA).

The TAC will remove or disable all access accounts for separated or terminated employees immediately following separation from the agency.

Primary responsibility for account management belongs to the Terminal Agency Coordinator (TAC). The TAC shall:

- Modify user accounts in response to events like name changes, accounting changes, permission changes, office transfers, etc.,
- Periodically review existing accounts for validity (at least once every 6 months), and
- Cooperate fully with an authorized security team that is investigating a security incident or performing an audit review.

F.1 Security Incident Response Form

**FBI CJIS DIVISION
INFORMATION SECURITY
OFFICER (ISO) SECURITY
INCIDENT REPORTING FORM**

NAME OF PERSON REPORTING THE INCIDENT: _____

DATE OF REPORT: _____ (mm/dd/yyyy)

DATE OF INCIDENT: _____ (mm/dd/yyyy)

POINT(S) OF CONTACT (Include Phone/Extension/Email): _____

LOCATION(S) OF INCIDENT: _____

INCIDENT DESCRIPTION: _____

SYSTEM(S) AFFECTED: _____

SYSTEM(S) AFFECTED (e.g. CAD, RMS, file server, etc.): _____

METHOD OF DETECTION: _____

ACTIONS TAKEN/RESOLUTION: _____

Copies To:

iso@nigc.gov

and

John C. Weatherly

(FBI CJIS Division ISO) 1000

Custer Hollow Road

Clarksburg, WV 26306-0102

(304) 625-3660

iso@fbi.gov

Appendix G

LOCAL AGENCY SECURITY OFFICER (LASO) BASIC RESPONSIBILITIES

RESPONSIBILITY	DESCRIPTION
Primary liaison	<p>Person through which all communication regarding audits, training, and security is conducted.</p> <p>First point of contact for NIGC in the event of an allegation of criminal history misuse or a security issue involving the background check process.</p>
Information Changes	Keeps information with NIGC current by informing the NIGC of any changes in the Tribe's information, the LASO, or the Authorized Tribal Signatory (submits the proper information change forms).
Authorized Personnel List	Submits and maintains a current Authorized Personnel List with the NIGC.
Privacy and Security Compliance	<p>Primarily responsible for agency compliance with all Privacy and Security rules.</p> <p>Maintains copies of Authorized Personnel Acknowledgement Statements and dissemination logs (if applicable).</p> <p>Ensures Tribe has adequate policies/procedures related to access, use, handling, dissemination, and destruction of CJ/CHRI.</p>
Training	<p>Ensures Authorized Personnel receive required agency-provided privacy and security training. Reviews Tribal training outlines to ensure topics are adequately covered.</p> <p>Ensures Authorized Personnel receive required standard online training.</p> <p>Updates Tribe training documentation as needed.</p>
Audits	<p>Cooperates with NIGC and/or federal officials during the audit process.</p> <p>Maintains all required audit documentation and serves as the Tribal representative for audits.</p> <p>Completes all documentation required during the audit and submits any required corrective action documentation in a timely manner.</p>

And

ISO@NIGC.GOV

Appendix H

Sample Noncriminal Justice Agency Information Change Form

Date	Agency Name	Agency ORI
-------------	--------------------	-------------------

Change/Add Contact Type: Check all that apply Local Agency Security Officer (LASO) <input type="checkbox"/> Applicant Team <input type="checkbox"/> Secondary LASO <input type="checkbox"/>	Previous Contact		
	New Contact Information		
	Title	Name	
	Phone	Fax	Email

Change Authorized Tribal Signatory	Previous Authorized Tribal Signatory Name		
	New Authorized Tribal Signatory Information		
	Title	Name	
	Phone	Fax	Email

Change Address: <input type="checkbox"/> Physical <input type="checkbox"/> Mailing <input type="checkbox"/>	Address Line 1		
	Address Line 2		
	City	State	Zip

Change Agency Name Previous Name: New Name:	Change Agency Main Phone New phone number:
--	--

Additional Comments/Information:	Leave Blank – NIGC use only
----------------------------------	-----------------------------

Name and Title of Person Submitting Form (Please Print Legibly):	
--	--

Send completed form to: National Indian Gaming Commission
 ATTN: Information Security Officer
 1849 C Street NW | Mail
 Stop 1621
 Washington, DC 20240

OR

Fax: (202-632-7066
 ATTN: Information Security Officer
 Email: iso@nigc.gov

Appendix I

Sample Authorized Personnel List

Name	Tribe Name	Commission or Casino Name	Department	Position	LASO Y/N	Email	Phone	Date Added	Date Termed
Jane Doe	AAA Tribe	XXX Gaming Commission	Licensing	Licensing Manager	Y	J.doe@abc.com	555-555-5555	1/25/2020	
John Doe			Licensing	Background Investigator	N	Ddoe@xyz.com		2/15/2020	
Bobby Smith			Commission	Commissioner	N	b.smith@abc.com	444-444-4444	1/1/2018	2/25/2020
Dan Smith		Lucky Casino	IT	IT Manager	N	Dan@luckycasino.net	123-45-6789	2/15/2020	

Notes:

- 1) Please list all Authorized Personnel who are authorized to receive, view, handle, disseminate, store, retrieve or dispose of CJ/CHRI. This includes having access to the fingerprint system.
- 2) Please document date an employee is no longer authorized to view/handle CJ/CHRI.
- 3) Please submit legal name changes and contact information updates if applicable.
- 4) If information is the same as the previous row, leave the information for the row blank

SAMPLE

ZYX Gaming Commission

123 Any Town Road
Your Town, AB 12345

May 1, 2020

National Indian Gaming Commission
1849 C Street NW
Mail Stop #1621
Washington, DC 20240

Dear NIGC Information Security Officer:

The following is an updated authorized personnel list for the ZYX Gaming Commission.

<u>Authorized Individual</u>	<u>Title</u>
Smith, John	Commissioner
Doe, Jane	Executive Director
Anderson, Sandy	Licensing Manager (LASO)
Jones, Sally	Licensing Agent
Thomas, Jack	IT Manager

If you have any questions, you can reach me at (800) 555-5555 Ext 1.

Sincerely,

Sandy Anderson
Local Agency Security Officer
Licensing Manager, ZYX Gaming Commission

Updated 2/24/2020

Appendix J

SAMPLE NONCRIMINAL JUSTICE AGENCY TRAINING DOCUMENTATION FORM

AGENCY NAME: _____ OCA: _____

The following training is REQUIRED:

Security Awareness Training (CJIS Online)

This training must be completed within 6 months of hire or appointment to position with access to criminal justice/criminal history record information. It must be repeated every two years for as long as the individual is on the agency Authorized Personnel List and granted access to criminal justice and/or criminal history record information.

Agency Internal Privacy and Security Training

Any personnel placed on the agency authorized Personnel List should receive internal agency training on the agency's security and handling processes prior to being allowed access to criminal justice and/or criminal history record information. Refresher training shall be completed every two years.

Name	First Time (F) or Refresher Training (R)?	Date of Security Awareness Training (CJIS online)	Date of Agency Privacy & Security Training	Acknowledgement Statement Signed? (Y/N)
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				

The persons named above have received the required training in accordance with applicable rules and regulations.

LASO Printed Name: _____ LASO Signature: _____ Date: _____

PLEASE PRINT LEGIBLY- Keep training logs on file. Training logs will be reviewed during audits. The National Indian Gaming Commission (NIGC) will also periodically request the agency submit training logs as part of quality assurance and compliance review. Please do not send training logs to the NIGC unless requested.

Appendix K

National Indian Gaming Commission Fingerprint MOU/CJIS Checklist

Tribe/TGRA:	Date:
NIGC Compliance Officer:	LASO:
Authority	
Under what authority does the TGRA access CHRI?	IGRA _____ State Statute _____ If yes, name/citation: _____ Other _____
Purpose	
Does the TGRA have an executed Memorandum of Understanding with the NIGC dated 2017 or later?	Yes _____ No _____
Have all Authorized Personnel who access CHRI received and reviewed the MOU?	Yes _____ No _____
Does your TGRA audit or review to ensure only fingerprint are submitted for employees of the gaming operation who are classified as Key Employees or Primary Management Officials as defined in 25 C.F.R. 502.14 (a-c) or 502.19 (a-c)? (Policy Required)	Yes _____ Method of verification _____ No _____
How does the TGRA background applicants who are classified as Key Employees or Primary Management Officials as defined in 25 C.F.R. 502.14 (d) or 502.19 (d)? (Policy Required)	Method Used _____ Approved gaming ordinance page, where the definitions of these PMOs and KEs are located: _____
Are there applicant positions that are no longer fingerprinted through the NIGC after the review?	Yes _____ List Positions _____ No _____
Are there applicant positions that require additional TGRA review or consideration by the NIGC?	Yes _____ List Positions _____ No _____
Are there applicant positions that are not classified as Key Employees or Primary Management Officials as defined in 25 C.F.R.	Yes _____ Provide Justification _____ No _____

502.14 (a-c) or 502.19 (a-c) which are still being fingerprinted?	
Fingerprint Submissions	
Are fingerprints processed through NIGC? *If yes, continue review. If no, completion of checklist is voluntary.	Yes _____ No _____
What methods are used to capture and submit fingerprints?	Hard Card Submission? _____ Electronic Submission? _____
Prior to fingerprinting the applicant, does the TGRA verify the identity of the individual being fingerprinted? (Policy Required)	Yes _____ By what means? _____ No _____
Prior to submitting fingerprints, does the TGRA notify the individual fingerprinted in writing ³ that the fingerprints will be used to check the Criminal History Records of the FBI (28 C.F.R. 50.12(b))?	Yes _____ No _____
Prior to submitting the fingerprints, does the TGRA ensure the applicant receives the FBI Privacy Act notice that is dated 2013 or later? (Policy Required)	Yes _____ No _____
Prior to submitting fingerprints, does the TGRA ensure the applicant receives the FBI Noncriminal Justice Applicants Rights Notice? (Policy Required)	Yes _____ No _____
Does the TGRA complete the Reason for Fingerprint (RFP) field to ensure the correct RFP is used? (INDIAN GAMING LICENSEE)	Yes _____ No _____
Does the TGRA submit fingerprints for other agencies? (Strictly Prohibited)	Yes _____ Which ones? _____ No _____
Receipt of Criminal History Record Information (CHRI)	
Does the TGRA receive CHRI results after the submission of a fingerprint-based transaction?	Yes _____ No _____
How does the TGRA receive the CHRI?	Mail (hard copy) _____ Email _____ Live Scan Device _____
Use of Criminal History Record Information (CHRI)	
For what purpose does the TGRA use the CHRI? (Policy Required)	Licensing _____ Employment _____ Other _____ Please describe: _____

³ Written notification includes electronic notification but excludes oral notification.

What other TGRA documents/situations contain CHRI or summary CHRI?	Notice of Results _____ Investigative Reports _____ Objection Letters _____ Spreadsheets _____	Phone Calls _____ Databases _____ Meeting Notes _____ Other _____
Is CHRI or summary CHRI reused for any other purpose after the initial inquiry?	Yes _____ No _____ If yes, Explain: _____	
Who has access to the CHRI? (Policy Required, Outsourcing Agreements may be required)	Licensing Staff _____ Other Department(s) (e.g., IT) _____ Other Agency Contractor(s) _____ Other _____	
Is CHRI or summary CHRI disseminated to or shared with any entity other than the NIGC?	Yes _____ No _____ If yes, explain who, when, and under what circumstances: _____	
Applicant Involvement		
Does the TGRA provide the applicant an opportunity to complete, or challenge the accuracy of, the information contained in the FBI identification record (28 C.F.R. 50.12 (b))? (Policy Required)	Yes _____ No _____	
If Yes to the above question, does the TGRA advise the applicant in writing ⁴ of the procedures for obtaining a change, correction, or update of an FBI identification record, as set forth in 28 C.F.R. 16.34 (DO Process)? (28 C.F.R. 50.12 (b)) (Policy Required)	Yes _____ If yes, describe how: _____ No _____	
Does the TGRA provide the applicant reasonable time to correct or complete the record (or decline to do so) before the TGRA takes action on their license or employment? (Policy Required)	Yes _____ How much time is provided? _____ No _____	
Does the TGRA choose to disseminate the applicant's CHRI record to the applicant? (Policy Required)	Yes _____ No _____	
If Yes to the above question, does the TGRA verify the applicant's identity prior to	Yes _____ How? _____ No _____	

⁴ Written notification includes electronic notification but excludes oral notification.

disseminating a copy to the applicant or their attorney working on their behalf?	
If Yes to the above question, does the TGRA document the release and mark the CHRI in a way to determine the document is a copy?	Yes _____ How? _____ No _____
If No to the above question, does the TGRA advise the applicants how to obtain the CHRI record from the FBI directly? (Policy Required)	Yes _____ No _____
Handling of Criminal History Record Information (CHRI)	
Does the TGRA have a retention policy/procedure for CHRI? (Policy Required)	Yes _____ No _____
Does the TGRA retain CHRI (hard copies or electronic), or documents containing CHRI or summaries of it? (Policy Required)	Yes _____ No _____
If the TGRA does retain CHRI, how long are they stored? (Policy Required)	Time _____
When retention of CHRI is no longer required, what is the method of disposal? (Policy Required)	Shred _____ Incinerate _____ Routine Trash _____ Overwriting 3 or more times _____ Degaussing _____ Other _____
Do Authorized Personnel complete the disposal of CHRI? (Policy Required)	Yes _____ No _____
If No to the above question, do Authorized Personnel oversee the CHRI destruction? (Policy Required)	Yes _____ No _____
Local Agency Security Officer Responsibilities	
Has the TGRA designated a Local Agency Security Officer (LASO)? (Policy Required)	Yes _____ No _____
Does the LASO update the Tribal and TGRA information with the NIGC if changes occur? (Policy Required)	Yes _____ No _____
Has the LASO submitted the Authorized Personnel List to the NIGC and submits updated lists as needed? (Policy Required)	Yes _____ No _____
Have all Authorized Personnel signed the Tribe's Acknowledgement Statement? (Policy Required)	Yes _____ No _____
Has the LASO completed training required	Yes _____ Through what means? _____

under CJIS Policy 5.2.2 prior to assuming the LASO duties and annually thereafter? (Policy Required)	No _____
Has the LASO ensured all Authorized Personnel have received FBI Security Awareness Training within 6 months of being placed on the Authorized Personnel List or their date of hire and every two years thereafter? (Policy Required)	Yes _____ Through what means? _____ No _____
Has the LASO ensured the Tribe has adequate policies and procedures related to access, use, handling, dissemination and destruction of CJI/CHRI? (Policies Required)	Yes _____ Please list the name of each: _____ No _____
Has the LASO ensured all Authorized Personnel have received internal training on approved policies and procedures regarding CHRI within 6 months of being placed on the Authorized Personnel List or their date of hire and every two years thereafter? (Policy Required)	Yes _____ No _____
Has the LASO implemented a security incident reporting policy which requires notification of findings be reported to the NIGC within 24 hours of detection? (Policy Required)	Yes _____ No _____
Does the LASO complete a training documentation form for the above trainings and retain the document for audit purposes? Are Security Awareness Training records maintained for a minimum of two years? (Policy Required)	Yes _____ No _____
Does the LASO audit to ensure each fingerprint submission is for the specific purpose of Key Employee and Primary Management official employments and is made pursuant to the authority to access the CHRI? (Policy Required)	Yes _____ No _____
Outsourcing Agreements	
Does the TGRA have an FBI Compact Council approved outsourcing agreements ⁵ for all entities with access to CHRI? (Policy Required)	Yes _____ No _____
Does the TGRA audit the entity's compliance	Yes _____

⁵ Such approval must be in writing and provided prior to the contracts being entered into or the entity accessing CJI or CHRI.

with the CJIS Security Policy within 90 days of entering the outsourcing agreement? (Policy Required)	No _____
Resource Documents	
Indian Gaming Regulatory Act	https://www.govinfo.gov/content/pkg/USCODE-2014-title25/pdf/USCODE-2014-title25-chap29.pdf
FBI CJIS Security Policy	https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center
Noncriminal Justice IT Security Audit	https://www.nigc.gov/compliance/CJIS-Training-Materials
FBI Security Awareness Training PowerPoint Presentation	https://www.nigc.gov/compliance/CJIS-Training-Materials
Draft Information Technology Security Policy Templates	https://www.fbi.gov/services/cjis/compact-council/sanctions-process-information
FBI Privacy Act Statement	https://www.fbi.gov/services/cjis/compact-council/privacy-act-statement
Noncriminal Justice Applicant's Privacy Rights Notice	https://www.fbi.gov/services/cjis/compact-council/guiding-principles-noncriminal-justice-applicants-privacy-rights
Outsourcing of Noncriminal Justice Functions Guide	https://www.nigc.gov/compliance/CJIS-Training-Materials
CJIS Contact Information	
Mr. Virgilio Congmon NIGC Information Security Officer iso@nigc.gov (202) 632-7003	Mr. Shea Bennett NIGC CJIS Systems Officer itsupport@ngic.gov (202) 632- 7003
Chasity S. Anderson FBI Compact Officer FBI / CJIS Division csanderson@fbi.gov (304) 625-2803 (office) (304) 476-3383 (mobile)	John C. Weatherly FBI CJIS ISO FBI/CJIS jcweatherly@fbi.gov (304) 625-3660 (office) (304) 709-1493 (mobile)

Updated 2/24/2020

**Noncriminal Justice Agency
(NCJA)
Information Technology
Security Audit
Correspondence Questionnaire**



Agency Contact Information

Please complete the following, where applicable only.

Audit Information:

Agency Name/Department Name: _____
ORI/Unique Identifier: _____
Name of Agency Head: _____ Title: _____
Mailing Address: _____

Primary Point of Contact (POC):

Name: _____ Title: _____
Street Address: _____ City: _____ State: _____ Zip: _____
Phone: _____ Alt. Phone: _____ Email: _____

Local Agency Security Officer (LASO) (technical POC, if applicable):

Name: _____ Title: _____
Street Address: _____ City: _____ State: _____ Zip: _____
Phone: _____ Alt. Phone: _____ Email: _____

Physical Address (main address where CHRI/CJI is accessed):

Contact Name: _____ Title: _____
Street Address: _____ City: _____ State: _____ Zip: _____
Phone: _____ Alt. Phone: _____ Email: _____

Data Center (if different from physical address):

Contact Name: _____ Title: _____
Street Address: _____ City: _____ State: _____ Zip: _____
Phone: _____ Alt. Phone: _____ Email: _____

Offsite Media Storage (where media containing CJI is stored outside of the agency):

Contact Name: _____ Title: _____
Street Address: _____ City: _____ State: _____ Zip: _____
Phone: _____ Alt. Phone: _____ Email: _____

Back-up Recovery Site (disaster recovery site/where system back-ups are stored):

Contact Name: _____ Title: _____
Street Address: _____ City: _____ State: _____ Zip: _____
Phone: _____ Alt. Phone: _____ Email: _____

AUTHORIZED USE/ACCESS TO CRIMINAL JUSTICE INFORMATION

*****Please note criminal history record information (CHRI) is a subset of criminal justice information (CJI) and are interchangeable for the purposes of this document.*****

1. Under what authority does the agency have access to national CHRI/CJI?

- State statute: _____
- NCPA/VCA
- Adam Walsh Act
- HUD (Housing and Urban Development) / PHA (Public Housing Authority)
- Real ID Act
- Other: _____

2. Does the agency have access to CHRI/CJI by means other than fingerprint submission?

- YES NO N/A

3. Describe the process for the submission of civil fingerprint transactions to include method of submission to the state Repository.

4. How does the agency receive or retrieve the national CHRI response from the state Repository?

- mail (hard copy)
- fax
- email
- website
- livescan device
- other: _____

RETENTION OF CRIMINAL JUSTICE INFORMATION

1. Does the agency retain the results (hard copies or electronic) of the criminal history record check or documents containing CHRI/CJI? YES NO N/A

- hard copy (case files, filing cabinet, etc.)
- e-mail (kept on email server/archive)
- scanned/saved to network share (more than one person can access)
- Excel spreadsheet (yes/no indicators kept, etc.)
- scanned/saved to desktop (not on network file share)
- website/internet application (records management system/personnel database, etc.)
- other: _____

2. Is the CHRI/CJI commingled (kept in same location) with any other records (such as in a personnel file with tax information, etc.)? YES NO N/A

DISSEMINATION OF CRIMINAL JUSTICE INFORMATION

1. Does the agency disseminate CHRI/CJI results to the individual of record or applicant? YES NO N/A

a. How is the information disseminated?

- mail (hard copy)
- courier service
- hand carried by authorized personnel
- email
- website/internet
- verbal (face to face or by phone)
- fax
- other: _____

2. Does the agency disseminate CHRI/CJI to any other entity/individual? YES NO N/A

a. Who?

- private contractors (for outsourcing – additional questions below)
- another similar agency (e.g. one school to another school)
- grant funded positions (give results to grant provider)
- accreditations (providing CHRI to accreditation company for review/proof)
- licensing
- audit (other than FBI/State Repository)
- other: _____
- other: _____

b. How is the CHRI/CJI shared?

- mail (hard copy)
- courier service
- hand carried by authorized personnel
- email
- website/internet
- Verbal (face to face or by phone)
- fax
- other: _____

c. What information is sent?

d. Why is the information sent/for what purposes would you disclose the results?

3. How is the information protected during dissemination?

- encryption (if via email, accessed via an internet website or application)
- tamper-proof container (sealed envelope, locked container, etc.)
- hand carried by authorized personnel
- certified mail
- other: _____

a. If CHRI/CJI is sent via email or accessed from an internet based application or website, please describe methods (bit level such as 128, hardware/software, etc.) of encryption and the National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 140-2 certification number.

b. Does the agency protect the information using a passphrase (to unlock encryption)? Please describe.

ADMINISTRATION OF NONCRIMINAL JUSTICE ADMINISTRATIVE FUNCTIONS

PRIVATE CONTRACTORS

1. Does the agency outsource (use private contractor personnel/vendors) for any noncriminal justice administrative functions that provides private contractor personnel with access to CHRI/CJI?

YES NO N/A

a. If YES, what noncriminal justice administrative functions are private contractors performing?

- data destruction (paper shredding, hard drives, etc.)
- IT services (network/system administrations, desktop support, etc.)
- off-site media storage (data centers, backup, paper storage archives, etc.)
- dispositions (obtains additional information from court of jurisdiction)
- hiring decisions (mails offer letters, generates security badges/credentials, etc.)
- scanning services (scans results into database or electronic file)
- other: _____

b. Has the agency obtained state/repository level approval for private contractor access to CHRI/CJI?

YES NO N/A

c. Has the agency designated someone as an Agency Coordinator to ensure all private contractor personnel have completed a fingerprint based record check (if applicable), completed the appropriate level security awareness training, and abide by all policies within the CJIS Security Policy?

YES NO N/A

- d. Does the agency have a contract/agreement with the private contractor(s), which incorporates or references the CJIS Security Policy and Outsourcing Standard? YES NO N/A

PERSONNEL SECURITY

1. Has the state passed legislation authorizing or requesting civil fingerprint-based record checks for personnel with access to CHRI/CJI for the purposes other than the administration of criminal justice functions (e.g., licensing and employment)? YES NO N/A
- a. If YES, has the agency ensured all personnel with unescorted access to CHRI/CJI have completed a state and national fingerprint-based record check within 30 days of access to CHRI/CJI? (should include agency personnel, IT staff, private contractors, cleaning/maintenance personnel with physical access to secure locations) YES NO N/A

SECURITY AWARENESS TRAINING

1. Does the agency ensure all personnel with unescorted access to CHRI/CJI have completed security awareness training within 6 months of assignments and at least every two years after? (should include agency personnel, IT staff, private contractors, cleaning/maintenance personnel with physical access to information) YES NO N/A
- a. If YES, is documentation of individual security awareness training maintained in a current status, to include private contractors if applicable? YES NO N/A
- b. Is the agency using the state provided training curriculum? (If NO, please provide training materials for review)
- YES NO N/A

SECURITY INCIDENTS AND VIOLATIONS

1. Does the agency provide and enforce the CJIS Security Policy to all authorized users, to include private contractor personnel? YES NO N/A
2. Does the agency have a written policy for the discipline of CJIS policy violators? YES NO N/A
3. What are the procedures when a security violation or incident is detected?
- _____
- _____
- _____
- a. Does the agency report the security violation or incident to anyone? Who? YES NO N/A
- _____
- _____
- _____
- b. Are all employees and/or private contractors made aware of the reporting procedures? YES NO N/A

- c. Are the procedures described above written in agency policy? YES NO N/A
4. Has the agency reported/had any security violations or incidents in the last 3 years? (incidents in which security of CHRI/CJI was compromised or put at risk) YES NO N/A

INFORMATION PROTECTION

*****Please note, if the agency does not retain criminal history record information or criminal justice information, the following sections are not applicable. Please skip each section that is not applicable and complete the signature block on the last page of this questionnaire before returning as indicated.*****

FOR HARD COPY STORAGE AND ACCESSIBILITY

The following questions apply to noncriminal justice agencies retaining all or part of the national criminal history record in paper (hard copy) form.

1. Describe all locations where and how criminal history record information is retained. (e.g. locked file cabinet, locked office, off-site storage facility, records archive, etc.)

2. Is the storage location physically secured? (i.e. unauthorized personnel cannot access CHRI/CJI, within a locked file with limited access, in a locked office, in a safe, etc.) YES NO N/A
 - a. Does the agency house files that contain CHRI/CJI in an off-site record storage facility? YES NO N/A
 - b. Who owns/manages the facility? (i.e. who controls access)

 - c. How are records transported to the off-site facility?

 - d. How are the records stored at the off-site facility?

3. Does the agency have a written policy that describes physical protections? (i.e. how and where the information must be stored, who can access, restricts unauthorized access, requires visitors to be escorted, etc.) YES NO N/A
4. Are visitors escorted by authorized personnel in physically secure locations at all times (in all access and storage areas to include off-site facilities if designated physically secure)? YES NO N/A

5. How does the agency dispose of physical (hard copy/paper) media containing CHRI/CJI?

- a. Does the agency have written procedures for paper destruction? YES NO N/A
- b. If the agency personnel does not conduct the sanitization or destruction of the media and it is performed by another entity, is the process witnessed by authorized personnel?
 YES NO N/A

FOR SINGLE DESKTOP STORAGE AND ACCESSIBILITY

The following questions apply to noncriminal justice agencies retaining all or part of the criminal history record on a single computer (desktop, laptop, tablet, etc.) that is not part of a larger shared network. (i.e. one user/one desktop)

1. What information is kept? (i.e. scanned copies, excel spreadsheet with CHRI/CJI indicators, word documents with descriptors, email account, etc.)

2. Describe the physical location where the computer with access to CHRI/CJI is housed. (e.g., locked office, reception area, etc.)

a. Is the computer's location physically secured? (i.e. unauthorized personnel cannot access CHRI/CJI, computer is not left unattended, visitors are escorted while in area, etc.) YES NO N/A

b. Is the CHRI/CJI encrypted at rest? YES NO N/A

c. If encryption is used, please describe methods (bit level, hardware/software, etc.) of encryption. (e.g. Adobe Pro, WinZip, TrueCrypt, etc.)

d. Does the agency protect the information using a passphrase (to unlock encryption)? Please describe.

3. Does the agency have a written policy that describes physical protections? (i.e. how and where the information/equipment must be stored, who can access, restricts unauthorized access, requires visitors to be escorted, etc.) YES NO N/A

4. When a computer reaches end of life (no longer works) or is to be replaced/upgraded, how does the agency destroy the hard drive?

a. Does the agency have written procedures for the sanitization and/or destruction of electronic media (hard drive, thumb drive, CDs, etc.)? YES NO N/A

b. If the agency personnel does not conduct the sanitization or destruction of the media and it is performed by another entity, is the process witnessed by authorized personnel?
 YES NO N/A

5. When logging onto the computer or before accessing CHRI/CJI does the user enter a password that utilizes secure password attributes? (at least 8 characters, numbers/letters, expires every 90 days, cannot reuse 10 previous passwords, and does not display when entered) YES NO N/A

6. Do users ever share their usernames, password, or passphrase (if applicable)? YES NO N/A

7. Does the computer initiate a session lock (require the user to re-enter password) after a maximum of 30 minutes of inactivity? YES NO N/A

a. If a user leaves the computer, do they log out of the computer or lock the screen?
 YES NO N/A

8. Does the agency apply routine patches and updates to all software and components? (i.e. Windows updates, virus protection patches, etc.) YES NO N/A

9. Does the computer storing CHRI/CJI have access to the internet? YES NO N/A

a. If **YES**, describe the boundary protection used to protect the computer. (i.e., hardware/software firewalls, proxies, gateways, guards, routers, etc.)

b. Does the agency enable virus protection at start-up and employ automatic scanning and updates? Please describe. YES NO N/A

10. Does someone within the agency stay up to date with relevant security alerts and advisories? YES NO N/A

FOR SHARED NETWORK STORAGE AND ACCESSIBILITY

The following questions apply to noncriminal justice agencies retaining all or part of the criminal history record on a shared closed-network platform (not accessible from internet webpage).

1. What information is kept? (i.e. scanned copies, excel spreadsheet with CHRI/CJI indicators, word documents with descriptors, emails, etc.)

2. Identify all locations where CHRI/CJI is either maintained (stored) or can be accessed (e.g., servers, offsite backups, primary offices, secondary locations, third party cloud storage, etc.)

- a. Are all locations where CHRI/CJI is either maintained/stored or accessed considered physically secured? (i.e. unauthorized personnel cannot access CHRI/CJI, computer is not left unattended, visitors are escorted while in area, etc.) YES NO N/A

- b. Describe physical security measures. (i.e. key card access, locked doors, etc.)

- c. Is the CHRI/CJI encrypted at rest? YES NO N/A

- d. Is the CHRI/CJI encrypted in transit? (accessed from secondary location, emailed, remotely accessed) YES NO N/A

- e. If encryption is used, please describe methods (bit level, hardware/software, etc.) of encryption. (e.g. Adobe Pro, WinZip, TrueCrypt, etc.)

- f. Does the agency protect the information using a passphrase (to unlock encryption)?

Please describe.

YES NO N/A

3. Does the agency have a written policy that describes physical protections? (i.e. how and where the information/equipment must be stored, who can access, restricts unauthorized access, requires visitors to be escorted, etc.) YES NO N/A

4. Is the CHRI/CJI backed up to off-site storage or a disaster recovery location? YES NO N/A

a. Who owns/manages the facility? (i.e. who controls access)

b. How are backup records transported to the secondary facility? (i.e. disc to disc with encryption or physical tapes encrypted or in locked box, etc.)

c. How are the records stored at the off-site facility?

5. When a computer reaches end of life (no longer works) or is to be replaced/upgraded, how does the agency destroy the hard drive?

a. Does the agency have written procedures for the sanitization and/or destruction of electronic media (hard drive, thumb drive, CDs, etc.)? YES NO N/A

b. If the agency personnel does not conduct the sanitization or destruction of the media and it is performed by another entity, is the process witnessed by authorized personnel?
 YES NO N/A

6. Before logging into the computer or before accessing CHRI/CJI, does the agency display a system use notification, a warning to the user that they are accessing sensitive information and informing of the possible consequences for misuse? YES NO N/A

7. When logging onto the computer or before accessing CHRI/CJI does the user enter a password that utilizes secure password attributes? (at least 8 characters, numbers/letters, expires every 90 days, cannot reuse 10 previous passwords, and does not display when entered) YES NO N/A

8. Do users ever share their usernames, passwords, or passphrase (if applicable)? YES NO N/A

9. Describe the agency's process for issuing user accounts, deleting/disabling user accounts, and periodic validation of user accounts:

a. Are these procedures written? YES NO N/A

10. Does the information system initiate a session lock (require the user to re-enter password) after a maximum of 30 minutes of inactivity? YES NO N/A

a. If a user leaves the computer, do they log out of the computer or lock the screen?
 YES NO N/A

11. Does the information system log: YES NO N/A

- successful and unsuccessful log on attempts
- successful and unsuccessful password changes
- successful and unsuccessful actions by privileged accounts (adding users, deleting users, etc.)
- successful and unsuccessful actions related to CHRI (delete records, edits of information, access to the record, etc.)

a. Does each logged event include: date, time, component (where it occurred), type of event, user, outcome (success or failure)? YES NO N/A

b. Does the agency check logs (who accessed CHRI/CJI, logged in, etc.) at least weekly?
 YES NO N/A

c. How long are logs kept?

12. Does the agency apply routine patches and updates to all software and components? (i.e. Windows updates, firewall patches, etc.) YES NO N/A

13. Describe the boundary protection used to protect the network. (i.e., hardware/software firewalls, proxies, gateways, guards, routers, etc.)

a. Is CHRI/CJI separated from non-CHRI/CJI related access? (i.e. can unauthorized users access shared folder or location of CHRI/CJI or is it separated in some way, such as a VLAN?)

Please describe. YES NO N/A

14. Does the agency utilize intrusion detection (IDS) or intrusion protection (IPS) tools?
 YES NO N/A

15. Can users access CHRI/CJI remotely? (i.e., access network from outside physically secure location, etc.) Please describe. (i.e. method/application, encryption used, etc.) Include details. (e.g., Citrix, VPN, GoToMyPC, LogMeIn, TeamViewer, etc.) YES NO N/A

16. Does the agency enable virus protection at start-up and employ automatic scanning and updates on all computers and servers storing or accessing CHRI/CJI? Please describe. (i.e. type and version)
 YES NO N/A

17. Does someone within the agency stay up to date with relevant security alerts and advisories? YES NO N/A

18. Does the agency host any CHRI/CJI in a virtualized environment? YES NO N/A

a. Please describe how CHRI information is protected in a virtual environment. (i.e. how is CHRI protected from unauthorized access – partitions, separate virtual NICs, different hosts from non-CHRI related systems or internet facing applications, etc.?)

FOR RECORD MANAGEMENT SYSTEMS/DATABASE STORAGE AND INTERNET ACCESSABILITY

The following questions apply to noncriminal justice agencies retaining all or part of the criminal history record in a records management system or database that is accessible through the internet.

1. What information is kept? (i.e. scanned copies, entered descriptor data, etc.)

2. What is the name of the application/website/database housing CHRI/CJI? (i.e. HR database, etc.)

3. Identify all locations where criminal history information/CJI is maintained/stored. (e.g., application/web servers, database storage, offsite backups, primary offices, secondary locations, third party cloud storage, etc.)

a. Are all locations where CHRI is either maintained/stored considered physically secured? (i.e. unauthorized personnel cannot access CHRI, computer is not left unattended, visitors are escorted while in area, etc.) YES NO N/A

b. Describe physical security measures. (i.e. key card access, locked doors, etc.)

c. Is the CHRI or CJI encrypted at rest? YES NO N/A

d. If encryption is used for data at rest, please describe methods (bit level, hardware/software, etc.) of encryption.

4. Does the agency have a written policy that describes physical protections? (i.e. how and where the information/equipment must be stored, who can access, restricts unauthorized access, requires visitors to be escorted, etc.) YES NO N/A

5. Is the CHRI/CJI backed up to off-site storage or a disaster recovery location? YES NO N/A

a. Who owns/manages the facility? (i.e. who controls access)

b. How are backup records transported to the secondary facility? (i.e. disc to disc with encryption or physical tapes encrypted or in locked box, etc.)

c. How are the records stored at the off-site facility?

6. When a computer/server, etc. reaches end of life (no longer works) or is to be replaced/upgraded, how does the agency destroy the hard drive?

a. Does the agency have written procedures for the sanitization and/or destruction of electronic media (hard drive, thumb drive, CDs, etc.)?

YES NO N/A

b. If the agency personnel does not conduct the sanitization or destruction of the media and it is performed by another entity, is the process witnessed by authorized personnel?

YES NO N/A

7. Before logging into the application or website to access CHRI/CJI, does the agency display a system use notification, a warning to the user that they are accessing sensitive information and informing of the possible consequences for misuse? YES NO N/A

8. When logging onto the application or website and accessing CHRI/CJI does the user and/or administrator enter a password that utilizes secure password attributes that includes all of the following characteristics? YES NO N/A

- length must be at least eight characters
- must contain letters and numbers or special characters
- not be the same as the user ID
- expire within a maximum of 90 days
- not allow the reuse of the last 10 passwords
- not display when entered

9. Do users or IT administrators ever share their usernames or passwords or have generic group accounts? YES NO N/A

10. Describe the agency's process for issuing user accounts, deleting/disabling user accounts, and periodic validation of user accounts:

a. Are these procedures written? YES NO N/A

11. Does the information system or application initiate a session lock (require the user to re-enter password) after a maximum of 30 minutes of inactivity? YES NO N/A

a. If a user leaves the computer, do they log out of the computer or lock the screen? YES NO N/A

12. Are the following events logged: YES NO N/A

- successful and unsuccessful log on attempts
- successful and unsuccessful password changes
- successful and unsuccessful actions by privileged accounts (adding users, deleting users, etc.)
- successful and unsuccessful actions related to CHRI (delete records, edits of information, access to the record, etc.)

a. Does each logged event include: date, time, component (where it occurred), type of event, user, outcome (success or failure)? YES NO N/A

b. If a security incident happened in relation to the release or misuse of CHRI/CJI, could you identify the individual who carried out the action and when? YES NO N/A

c. Does the agency check logs (who accessed CHRI/CJI, logged in, etc.) at least weekly? YES NO N/A

d. How long are logs kept?

13. Does the agency apply routine patches and updates to all software and components? (i.e. Windows updates, firewall patches, etc.) YES NO N/A

14. Describe the boundary protection used to protect the network. (i.e., hardware/software firewalls, proxies, gateways, guards, routers, etc.)

a. Is CHRI/CJI separated from non-CHRI/CJI related access? (i.e. can unauthorized users access application or locations of CHRI/CJI or is it separated in some way, such as a VLAN?)

Please describe. YES NO N/A

15. Does the agency utilize intrusion detection (IDS) or intrusion protection (IPS) tools?
 YES NO N/A

16. How is CHRI/CJI encrypted when transmitted outside the physically secure location where it is stored? (i.e., how is the data encrypted when a user is accessing from an internet connection, etc.) Include details. (e.g., methods of encryption, bit level, hardware/software/application, FIPS certificate numbers, etc.)

17. Does the agency enable virus protection at start-up and employ automatic scanning and updates on all computers and servers storing or accessing CHRI/CJI? Please describe. (i.e. type and version)
 YES NO N/A

18. Does someone within the agency stay up to date with relevant security alerts and advisories?
 YES NO N/A

19. Does the agency host any CHRI/CJI in a virtualized environment? YES NO N/A

a. Please describe how CHRI information is protected in a virtual environment. (i.e. how is CHRI protected from unauthorized access – partitions, separate virtual NICs, different hosts from non-CHRI related systems or internet facing applications, etc.)

Before returning this audit, please complete the following information:

Questionnaire Completed By (signed name): _____

Questionnaire Completed By (print name): _____

Phone Number: _____ Date Completed: _____

E-mail address: _____

After completed, please attach all supporting documentation and send to the following:

Attention: _____

Phone: _____ Fax: _____

Email: _____

Mailing Address: Street: _____

City: _____ State: _____ Zip: _____

******* FOR OFFICIAL USE ONLY*******

Auditor Review

Auditor Name: _____ Date of Review: _____

Comments/Documents Provided/Notes: _____

Secondary Reviewer: _____ Date of Review: _____

Additional Comments: _____

Appendix L

Key Employee/ Primary Management Official Classification Guide for CHRI MOU Compliance

Under the 2020 Memorandum of Understanding (MOU) with the FBI, the National Indian Gaming Commission (NIGC) agrees to use CHRI solely for the purpose of determining an applicant's eligibility for employment as a key employee or primary management official at the Tribe's gaming operation, as defined in NIGC regulations, **25 C.F.R. §§ 502.14(a) – (c) and 502.19(a) – (c)**, and not for any other purpose.⁶

If a Tribe has an executed MOU with the NIGC, Tribes are permitted to submit fingerprints to the FBI through the NIGC to obtain and use Criminal History Record Information (CHRI) for the sole purpose of making an employment and/or licensing determination of KEs and PMOs as defined in the FBI/NIGC MOU. The NIGC offers the following technical assistance to tribal gaming regulatory authorities (TGRAs) for determining whether an applicant meets the definitions in the FBI/NIGC MOU.

Though there are some limitations, the position title can be an important indicator as to whether or not a gaming operation employee is a KE or a PMO. The proper classification of a gaming operation employee, however, depends upon the specific duties and responsibilities of the individual in their job/position. For example, a Food and Beverage Manager, as an employee of a gaming operation with an annual compensation of \$47,000, without the ability to hire or fire employees, who does not handle cash or gaming supplies, is not a KE. But if the same Food and Beverage Manager gets a raise and makes in excess of \$50,000 in a year, becomes a KE. Another example is Environmental Services (EVS) staff. In general, EVS staff are employees of a gaming operation with individual "total cash compensation" less than \$50,000 a year. Nevertheless, if when the TGRA examines the individual's specific duties and determines that the night-shift EVS employee performs additional duties normally completed by a KE, the EVS employee is a KE. These duties must include one or more listed in NIGC regulation, 25 C.F.R. § 502.14 (a)-(c), such as accessing or handling gaming equipment, gaming revenue, or gaming revenue accounting records (including revenue records in gaming equipment). Once an employee's position transforms into a KE position, the employee must go through the KE licensing process and their fingerprints may be submitted through NIGC for purposes of receiving their criminal history record.

To ensure CHRI MOU compliance, Tribes with an executed MOU are required to determine whether applicants meet the FBI/MOU definitions of a KE or a PMO prior to submitting fingerprints through the NIGC. The following questions should help guide the TGRA to properly classify such applicants. If additional analysis or further guidance is needed, please contact NIGC region staff.

Questions for KE Classification

⁶ 25 CFR §§502.14(d) and 502.19(d) are not categories of key employees and primary management officials whose prints can be submitted to the FBI through the NIGC MOU. However, the tribe can continue to license these categories through the NIGC if the tribe has an alternative, legal source of FBI CHRI other than the NIGC such as a statutory authorized tribal, state, local or 3rd party contractor.

1. Is the person an applicant or employee of the gaming operation?⁷
 - If yes, proceed to question two.
 - If no, the person cannot be fingerprinted because they do not satisfy the initial criterion of being an applicant or employee of a gaming operation.

2. An applicant or employee of a gaming operation whose “total cash compensation” will be or is in excess of \$50,000 per year?⁸
 - If yes, the person can be fingerprinted as a KE.
 - If no, proceed to the next question.

3. Is the person one of the “four most highly compensated persons in the gaming operation?”
 - If yes, the person can be fingerprinted as a KE.
 - If no, proceed to the next question.

4. A person in a position or performs duties that meet the definitions of a KE in accordance with NIGC regulation, 25 C.F.R. § 502.14 (a) through (c)?
 - If yes, the person can be fingerprinted as a KE.
 - If no, proceed to the next question.

5. Does the person watch, protect, handle, use, or maintain gaming cash and/or gaming revenue⁹?
Gaming cash means money used in the operation of Class II and III gaming. This includes cash deposited or withdrawn from the gaming operation’s cage or vault, in its kiosk and atms, gaming machine/system bill acceptors, drop boxes, change boxes, tip boxes, or other locations, containers, and devices used to store or retrieve cash used for the conduct of Class II and III games or accounted for as a cash asset of the gaming operation. The fact valet, housekeeping, wait staff, and other employees not involved in the conduct of gaming routinely receive tips and place them in a tip box would not require them to be licensed, but the person collecting and depositing the cash tips in the gaming operation’s cage/vault who takes on responsibility for an asset on behalf of the gaming operation qualifies as a KE.
 - If yes, the person can be fingerprinted as a KE.
 - If no, proceed to the next question.

⁷ See NIGC regulation, § 502.10, defining *Gaming operation*.

⁸ This includes all employees on the gaming operation’s payroll, full-time or part-time. Is the employee’s compensation listed as an operating expense on the gaming operation’s general ledger? Does the gaming operation issue a W-2 to the employee? Is the employee subject to the gaming operations employee handbook, rules and leave policy? In some circumstances, all tribal employees are paid through the tribe and follow the tribal employee handbook, including gaming operation employees. Examination of organization charts maintained by the gaming operation or tribal business entities will assist in making a determination. Does the employee and/or their supervisor report to the gaming operation’s general manager or executive officer? Examining the process under which the employee was hired can be helpful. Were they processed through something other than the gaming operations HR department?

⁹ See NIGC regulation, § 502.16, defining *Net gaming revenue*

6. Is the person a custodian of gaming supplies? This may include but is not limited to a person with access to gaming systems, machine ticket paper, chips, tokens, playing cards, bingo paper, bingo balls, or hardware/software used in conjunction with the Class II/III gaming systems.
 - If yes, the person can be fingerprinted as a KE.
 - If no, proceed to the next question.

7. Does the person have the ability to access and/or make changes to the gaming operation's accounting system, player tracking system, or gaming system record? This may include but is not limited to a person "with access to cash and accounting records," including accounting records within gaming equipment and devices.
 - If yes, the person can be fingerprinted as a KE.
 - If no, proceed to the next question.

8. Does the person have duties or responsibilities that include oversight of any portion of a gaming operation?¹⁰ Oversight duties or responsibilities may include but are not limited to manager-on-duty obligations.
 - If yes, the person can be fingerprinted as a KE.
 - If no, proceed to the next question.

9. Does the person perform the function of bingo caller, count room supervisor, chief of security, floor manager, pit boss, dealer, croupier¹¹, or approver of credit?
 - If yes, the person can be fingerprinted as a KE.
 - If no, proceed to the next question.

10. Does the person have any job functions or responsibilities that require the person to watch, touch, guard, count, maintain, or otherwise be responsible for gaming cash, gaming revenue, or gambling supplies/devices that has not already been discussed? The responsibilities may include accessing or modifying a Class II/III gaming system, player tracking system, or any other ancillary system that is integral to the play of the games or generation, collection, or recording of gaming revenue.
 - If yes, the person can be fingerprinted as a KE.
 - If no, the individual is not a KE.

Questions for PMO Classification

1. Is the person an applicant or an employee of a gaming operation or a management contractor?
 - If yes, proceed to question two.
 - If no, the individual cannot be fingerprinted unless they can be classified as a KE in the previous section.

2. Does the person have management responsibility for a gaming operation, facility, or part of either due to a management contract?

¹⁰ See NIGC regulation, § 502.10, defining *Gaming operation*.

¹¹ Croupier is an employee of a gambling casino who collects and pays bets and assists at the gaming tables.

- If yes, the person can be fingerprinted as a PMO.
 - If no, proceed to next question.
3. Does the person have the ability “to hire or fire employees?”
- If yes, the person can be fingerprinted as a PMO.
 - If no, proceed to next question.
4. Does the person “set up working policy for the gaming operation?”¹² This can include, but is not limited to, actions that direct a person to perform operational, administrative, or financial functions for a gaming operation.
- If yes, the person can be fingerprinted as a PMO.
 - If no, proceed to next question.
5. Does the person plan, organize, or coordinate the activities of gaming operation/management contractor employees at the gaming operation?
- If yes, the person can be fingerprinted as a PMO.
 - If no, proceed to next question.
6. Is the person “the chief financial officer or other person who has financial management responsibility for the operation?”
- If yes, the person can be fingerprinted as a PMO.
 - If no, the person is not a PMO.

Please note: The definition of key employee and primary management official has not changed. The FBI and FBI/NIGC MOU have clarified which KE and PMO applicant fingerprints can be submitted through the NIGC under the MOU.

¹² See NIGC Bulletin 1994-5, *Approved Management Contracts v. Consulting Agreements* (Oct. 14, 1994) (describing what are management functions and duties), <https://www.nigc.gov/images/uploads/bulletins/1994-5mgmtvconsult.pdf>

Appendix M



BULLETIN

No. 2020-2

February 18, 2020

Subject: Fingerprint processing - applicant Privacy Act rights and protecting CHRI

The NIGC processes fingerprints submitted by tribes for background investigations of primary management officials (PMO) and key employees (KE). Prior to issuing a gaming license to a PMO or KE, a tribe is required to perform a fingerprint check through the FBI records system as part of the background investigation on each applicant. The criminal history record information (CHRI) obtained as a result of the check assists the tribe in determining the applicant's eligibility for employment.

This bulletin discusses the requirements for fingerprint processing: notifying applicants of their Privacy Act rights, their opportunity to complete or challenge information in their FBI identification record, and the process by which they may obtain a change, correction, or update to such record. This bulletin also details the requirements for protecting and using CHRI, including summaries of it, and complying with the FBI's CJIS Security policy. The FBI and/or NIGC will audit Tribes' compliance with these requirements as set forth here and in each Tribe's Memorandum of Understanding (MOU) with the NIGC.

Applicant Privacy Act rights

1. *Applicant record notification / NCJA Privacy rights notice*

Prior to taking a PMO/KE applicant's fingerprints, tribes must provide these applicants with the written *Applicant Record Notification* - also known as the Non-Criminal Justice Applicant's Privacy Rights notice. It may be given to the applicant electronically or in paper form. A copy of the notice is attached to this Bulletin.

This notice includes multiple requirements. First, it explains that the applicant's fingerprints will be used to check FBI's criminal history records. Second, if a criminal history record exists concerning the applicant, the TGRA needs to give them an opportunity to complete or challenge the information in the record. Third, the TGRA has to advise the applicant in writing that the procedures for obtaining a change, correction, or update of the record are set forth in Title 28, Code of Federal Regulations (C.F.R.) §16.34. Finally, the TGRA must afford the applicant a

reasonable amount of time to correct or complete the record (or decline to do so) before denying a gaming license based on information in the record.¹

To facilitate the challenge/correction process, NIGC permits TGRAs to supply the applicant with a copy of their FBI criminal history record for review and possible challenge, correction, or update. This courtesy saves the applicant the time and additional fee required in obtaining the record directly from FBI. As a prerequisite, however, TGRAs must develop a written procedure for such releases. This written procedure must require verification of the applicant's identity prior to dissemination and must document each release. To limit potential risks associated with an applicant's subsequent use of CHRI, TGRAs need to mark the record in some manner to distinguish it as a copy, not the original. Although the preferred method is to release CHRI directly to the applicant, the record may be released, at the request of the applicant, to an attorney acting on their behalf. This scenario could arise as part of a formal appeal process, when an applicant challenges the outcome of the TGRA's eligibility determination. CHRI may not be disseminated to spouses or other household or family members, even at the applicant's request. And CHRI may not be disseminated to other parties such as potential employers or licensing agencies on behalf of the applicant.

If, however, the TGRA chooses not to provide the applicant a copy of the record, the TGRA's policy should prohibit its release for such purpose. And that policy must direct the applicant to the FBI's process for obtaining a copy, which is set forth at 28 C.F.R. §§16.30 - 16.34 and on the FBI's website, <https://www.fbi.gov/services/cjis/identity-history-summary-checks>.

2. FBI Privacy Act Statement

Also prior to submitting their fingerprints, PMO/KE applicants shall receive the FBI's Privacy Act Statement. The FBI's Privacy Act Statement is separate from the Privacy Act notice required under NIGC regulations², and a copy is attached to this Bulletin. Essentially, it informs applicants that their fingerprints will be used to check their criminal history records at the FBI.

3. Both must be provided before fingerprinting

Regardless of what entity a TGRA uses to submit fingerprints to the FBI, NIGC, or another source, the FBI requires that the Applicant Record Notification / NCJA Privacy rights notice and the FBI Privacy Act Statement be provided to all PMO/KE applicants prior to the applicant providing their fingerprints for a national criminal history records search.

FBI may update these notices periodically. Please check FBI's website for updates of the notices:

<https://www.fbi.gov/services/cjis/compact-council/privacy-act-statement>

<https://www.fbi.gov/services/cjis/compact-council/guiding-principles-agency-privacy-requirements-for-noncriminal-justice-applicants>

¹ See 28 C.F.R. § 50.12(b).

² 25 C.F.R. § 556.2.

CHRI Use and Protection

1. CHRI

CHRI means information collected by criminal justice agencies about individuals, consisting of identifiable descriptions and notations of arrests, detentions, indictments, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, and release.

CHRI also includes information that is transferred or reproduced directly from CHRI or information that confirms the existence or nonexistence of CHRI. CHRI includes any media that contains it, such as: Letters, emails, documents, notes, conversations – in person or via phone/text, and spreadsheets or tables. Examples of CHRI potentially include: notice of results (NORs), investigative reports (IRs), licensing objection letters, and other summaries of CHRI.

2. Using and protecting CHRI

CHRI is highly sensitive information – tribes, therefore, must take steps to ensure that it is used only for authorized purposes and securely maintained. CHRI may only be used to determine a PMO/KE applicant's eligibility for employment in the tribe's gaming operation, not for any other purpose. To be clear, "official use" of CHRI for licensing purposes is limited to those individuals performing work functions for, or managing, the gaming operation who come within the NIGC regulatory definitions of a PMO or KE, as set forth in 25 C.F.R. §§ 502.14 (a) – (c) and 502.19 (a) – (c).

All CHRI access must be restricted to tribal personnel directly involved in the licensing deliberations. And tribes shall maintain records of all persons accessing CHRI, which will be furnished to NIGC upon request. CHRI cannot be improperly disseminated beyond tribal personnel directly involved in licensing deliberations or reused.

Regarding reuse, CHRI obtained under an NIGC MOU cannot be shared with state gaming agencies for state licensing purposes. In most instances, CHRI made available via NIGC fingerprinting cannot be provided to tribal leadership, other tribal agencies beyond the TGRA, human resources, etc., to save money or to meet tribal-state gaming compact requirements. And although the use of CHRI may be necessary, and authorized under separate authority, to satisfy state licensing requirements, a new record request to the FBI through a non-NIGC process must be made in such instance.

However, regulatory inspections by a state gaming agency where they access CHRI as part of an audit or review of licensing during a site visit is not reuse and not prohibited. Neither are reviews by agencies that require residual access based on oversight and authority, such as an inspector general's office reviewing case files. But such access should be limited to only the minimum level necessary to accomplish oversight responsibilities and controls should be established to reasonably prevent unauthorized CHRI disclosure. Similarly, CHRI and its summary information may be disclosed in tribal proceedings related to KE/PMO eligibility determinations, but not in courts or administrative hearings without NIGC's prior consent.

3. FBI's CJIS Security policy and compliance audits

The FBI's Criminal Justice Information Services (CJIS) Division issued the CJIS Security policy to protect Criminal Justice Information³ (CJI) and, its subset, CHRI. The policy applies to every individual and entity accessing CJI and CHRI, detailing operational and information security requirements for protecting transmissions and storage of it - including the hardware, software, and infrastructure used to receive, transmit, and store it. The policy also contains directives on how CJI and CHRI shall be maintained, viewed, accessed, processed, released, and destroyed and the training and authorizations needed for those individuals that do so.

All tribes accessing CHRI through NIGC must agree to comply with the policy and implement its requirements as detailed in their NIGC MOUs and the policy itself. Tribes will be subject to annual audits, including information technology security audits, by the NIGC to ensure compliance with the NIGC MOU and the FBI's CJIS Security policy. The FBI may also audit the Tribes, and such audits would likely occur once every three years.

Training

The NIGC has updated its training modules for backgrounding, licensing, and understanding CHRI. It includes the definitions of CHRI, applicants' rights, CHRI use, and CHRI reuse. It also includes CJIS Security Awareness training, which is required under the CJIS Security policy. Please see the CJIS Training materials on the NIGC website:

<https://www.nigc.gov/compliance/CJIS-Training-Materials> . And a video entitled "NIGC Fingerprint Program Updates" covers information about updates to the NIGC fingerprint process and to the tribal background and licensing process, as well as the handling of FBI CHRI:

<http://bit.ly/CJISvideo>

New MOU

In order to ensure compliance with the above requirements, each tribe receiving CHRI via the NIGC has to execute a new Memorandum of Understanding (MOU) - on or before January 1, 2021. Like the current MOU, the new one limits CHRI's use, including any summary of it, to tribal eligibility determinations for KE/PMO employment. As always, the new MOU, similar to the old, underscores FBI's right to impose additional restrictions on the release and use of CHRI beyond those set by the NIGC and reserves NIGC's right to discontinue providing CHRI where a tribe fails to comply with the MOU's terms.

³ CJI is the term used for FBI CJIS provided data necessary for law enforcement and civil regulatory agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data.

Appendix N

Tribe Name

Determination of Eligibility/Suitability & Notification of Results to NIGC
(25 USC 2710 & 25 CFR 558.2)

I. APPLICANT INFORMATION

Employee Name _____ SSN _____ DOB _____

Date Hired _____ or Date transferred to Key or Mgmt. Position _____

Applicant Status: Key Employee Primary Management Official Other Position _____

II. SYNOPSIS OF BACKGROUND INVESTIGATION CONDUCTED

- Current Address & Residence History (previous 5 years) Credit Check
- Past Employment Proof of Self-employment
- Personal Character References Tribal and/or District Court Record Check
- Criminal History Verified existing and previous relationships with Indian Tribes and the gaming industry.

The criminal history investigation revealed:

- No record.
- Every known criminal charge brought against the applicant within the last 10 years of the date of application:

- Every felony of which the applicant has been convicted or any ongoing prosecution.

OTHER GAMING LICENSES VERIFIED

- Gaming licenses previously denied: _____
- Gaming licenses revoked, even if subsequently reinstated _____
 - Employee has never applied for another gaming license Employee has applied for previous gaming license
 - Licensing agency: _____ License Status & Position: _____
 - Licensing agency: _____ License Status & Position: _____

III. ELIGIBILITY DETERMINATION

Based upon the information reviewed and the investigative findings and taking into consideration the applicant's prior activities, criminal record, if any, reputation, habits and associations, the _____ Gaming Commission has determined that the above named individual:

- Should be **granted** a gaming license
- Should be granted a **conditional** gaming license for a period of _____ months.
Condition _____
- Should be **denied** a gaming license.
 - Did not fully and correctly fill out their Tribal License application as required
 - Other _____
- Has had their license **revoked** for cause (Please attach a summary of cause for revocation)
Revoked for _____
- Not licensed by the Tribe
- Notes related to the above determination if needed: _____

Authorized Tribal Official

Date

**National Crime Prevention
and Privacy Compact Council**



**Security and
Management Control
Outsourcing Standard
for Non-Channelers**

Approved by the Council on
May 16, 2018

SECURITY and MANAGEMENT CONTROL OUTSOURCING STANDARD for NON-CHANNELERS

The goal of this document is to provide adequate security and integrity for criminal history record information (CHRI) while under the control or management of an outsourced third party, the Contractor. Adequate security is defined in Office of Management and Budget Circular A-130 as “security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.”

The intent of this Security and Management Control Outsourcing Standard (Outsourcing Standard) is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the FBI Criminal Justice Information Services (CJIS) Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

This Outsourcing Standard identifies the duties and responsibilities with respect to adequate internal controls within the contractual relationship so that the security and integrity of the Interstate Identification Index (III) System and CHRI are not compromised. The standard security program shall include consideration of site security, dissemination restrictions, personnel security, system security, and data security.

The provisions of this Outsourcing Standard are established by the Compact Council pursuant to 28 CFR Part 906 and are subject to the scope of that rule. They apply to all personnel, systems, networks, and facilities supporting and/or acting on behalf of the Authorized Recipient to perform noncriminal justice administrative functions requiring access to CHRI without a direct connection to the FBI CJIS Wide Area Network (WAN).

1.0 Definitions

- 1.01 *Access to CHRI* means to view or make use of CHRI obtained from the III System but excludes direct access to the III System by computer terminal or other automated means by Contractors other than those that may be contracted by the FBI or state criminal history record repositories or as provided by Title 34, United States Code (U.S.C.), Section 40314 (b), (formally cited as 42 U.S.C. § 14614(b)).
- 1.02 *Authorized Recipient* means (1) a nongovernmental entity authorized by federal statute or federal executive order to receive CHRI for noncriminal justice purposes, or (2) a government agency authorized by federal statute, federal executive order, or state statute which has been approved by the United States Attorney General to receive CHRI for noncriminal justice purposes.

- 1.03 *Chief Administrator* means the primary administrator of a Nonparty State’s criminal history record repository or a designee of such administrator who is a regular full-time employee of the repository, which is also referred to as the State Identification Bureau (SIB) Chief.
- 1.04 *CHRI*, as referred to in Article I(4) of the Compact, means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, or release; but does not include identification information such as fingerprint records if such information does not indicate involvement of the individual with the criminal justice system.
- 1.05 *Criminal History Record Check*, for purposes of this Outsourcing Standard only, means an authorized noncriminal justice fingerprint-based search of a state criminal history record repository and/or the FBI system.
- 1.06 *Compact Officer*, as provided in Article I(2) of the Compact, means (A) with respect to the Federal Government, an official [FBI Compact Officer] so designated by the Director of the FBI [to administer and enforce the compact among federal agencies], or (B) with respect to a Party State, the chief administrator of the State’s criminal history record repository or a designee of the chief administrator who is a regular full-time employee of the repository.
- 1.07 *Contractor* means a government agency, a private business, non-profit organization or individual, that is not itself an Authorized Recipient with respect to the particular noncriminal justice purpose, who has entered into a contract with an Authorized Recipient to perform noncriminal justice administrative functions requiring access to CHRI.
- 1.08 *Dissemination* means the disclosure of CHRI by an Authorized Recipient to an authorized Contractor, or by the Contractor to another Authorized Recipient consistent with the Contractor’s responsibilities and with limitations imposed by federal and state laws, regulations, and standards as well as rules, procedures, and standards established by the Compact Council and the United States Attorney General.
- 1.09 *Identity History Summary (IdHS)*, for the purposes of this Outsourcing Standard, means the report of all identification, demographic, and event information (criminal and/or civil) within a Next Generation Identification (NGI) Identity record which may be disseminated to an Authorized Recipient contingent upon legislation and federal regulations. The IdHS contains the criminal justice information associated with criminal fingerprint (i.e., “rap sheets”) and/or noncriminal justice information associated with the civil fingerprints, therefore the existence of an IdHS

alone does not reflect criminal history events on that NGI Identity. This term is unique to NGI and is not intended to affect other agencies' use of the term "rap sheet" to describe reports of information in their identification repositories.

- 1.10 *Noncriminal Justice Administrative Functions* means the routine noncriminal justice administrative functions relating to the processing of CHRI, to include but not limited to the following:
 1. Making fitness determinations/recommendations
 2. Obtaining missing dispositions
 3. Disseminating CHRI as authorized by Federal statute, Federal Executive Order, or State statute approved by the United States Attorney General
 4. Other authorized activities relating to the general handling, use, and storage of CHRI
- 1.11 *Noncriminal Justice Purposes*, as provided in Article I(18) of the Compact, means uses of criminal history records for purposes authorized by federal or state law other than purposes relating to criminal justice activities, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.
- 1.12 *Outsourcing Standard* means a document approved by the Compact Council after consultation with the United States Attorney General which is to be incorporated by reference into a contract between an Authorized Recipient and a Contractor. This Outsourcing Standard authorizes access to CHRI for noncriminal justice purposes, limits the use of the information to the purposes for which it is provided, prohibits retention and/or dissemination except as specifically authorized, ensures the security and confidentiality of the information, provides for audits and sanctions, provides conditions for termination of the contract, and contains such other provisions as the Compact Council may require.
- 1.13 *Personally Identifiable Information (PII)* means information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name.
- 1.14 *Physically Secure Location* means a facility or an area, a room, or a group of rooms, within a facility with both the physical and personnel security controls sufficient to protect CHRI and associated information systems.
- 1.15 *PII Breach* means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access or any similar term referring to situations where persons other than the authorized users, and for other

than authorized purposes, have access or potential access to PII, whether physical or electronic.

- 1.16 *Positive Identification*, as provided in Article I(20) of the Compact, means a determination, based upon a comparison of fingerprints¹ or other equally reliable biometric identification techniques, that the subject of a record search is the same person as the subject of a criminal history record or records indexed in the III System. Identifications based solely upon a comparison of subjects' names or other non-unique identification characteristics or numbers, or combinations thereof, shall not constitute positive identification.
- 1.17 *Public Carrier Network* means a telecommunications infrastructure consisting of network components that are not owned, operated, and managed solely by the agency using that network, i.e., any telecommunications infrastructure which supports public users other than those of the agency using that network. Examples of a public carrier network include but are not limited to the following: Dial-up and Internet connections, network connections to Verizon, network connections to AT&T, ATM Frame Relay clouds, wireless networks, wireless links, and cellular telephones. A public carrier network provides network services to the public; not just to the single agency using that network.
- 1.18 *Security Violation* means the failure to prevent or failure to institute safeguards to prevent access, use, retention, or dissemination of CHRI in violation of: (A) Federal or state law, regulation, or Executive Order; or (B) a rule, procedure, or standard established by the Compact Council and the United States Attorney General.

2.0 *Responsibilities of the Authorized Recipient*

- 2.01 Prior to engaging in outsourcing any noncriminal justice administrative functions, the Authorized Recipient shall: (a) Request and receive written permission from (1) the State Compact Officer/Chief Administrator² or (2)

¹ The Compact Council currently defines positive identification for noncriminal justice purposes as identification based upon a qualifying ten-rolled or qualifying ten-flat fingerprint submission. Further information concerning positive identification may be obtained from the FBI Compact Council office.

²The Compact Officer/Chief Administrator may not grant such permission unless he/she has implemented a combined state/federal audit program to, at a minimum, triennially audit a representative sample of the Contractors and Authorized Recipients engaging in outsourcing with the first of such audits to be conducted within one year of the date the Contractor first receives CHRI under the approved outsourcing agreement. A representative sample will be based on generally accepted statistical sampling methods.

the FBI Compact Officer³; and (b) provide the State Compact Officer/Chief Administrator or the FBI Compact Officer copies of the specific authority for the outsourced work, criminal history record check requirements, and/or a copy of relevant portions of the contract as requested.

- 2.02 The Authorized Recipient shall execute a contract or agreement prior to providing a Contractor access to CHRI. The contract shall, at a minimum, incorporate by reference and have appended thereto this Outsourcing Standard.
- 2.03 The Authorized Recipient shall, in those instances when the Contractor is to perform duties requiring access to CHRI, specify the terms and conditions of such access; limit the use of such information to the purposes for which it is provided; limit retention of the information to a period of time not to exceed that period of time the Authorized Recipient is permitted to retain such information; prohibit dissemination of the information except as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General; ensure the security and confidentiality of the information to include confirmation that the intended recipient is authorized to receive CHRI; provide for audits and sanctions; provide conditions for termination of the contract; and ensure that Contractor personnel comply with this Outsourcing Standard.
- a. The Authorized Recipient shall conduct criminal history record checks of Contractor personnel having access to CHRI if such checks of the Authorized Recipient's personnel are required or authorized under an existing federal statute, executive order, or state statute approved by the United States Attorney General under Public Law 92-544.⁴ The Authorized Recipient shall maintain updated records of Contractor personnel who have access to CHRI and update those records within 24 hours when changes to that access

³State or local Authorized Recipients based on State or Federal Statutes shall contact the State Compact Officer/Chief Administrator. Federal or Regulatory Agency Authorized Recipients shall contact the FBI Compact Officer.

⁴If a national criminal history record check of Authorized Recipient personnel having access to CHRI is mandated or authorized by a federal statute, executive order, or state statute approved by the United States Attorney General under Public Law 92-544, the State Compact Officer/Chief Administrator and/or the FBI Compact Officer must ensure Contractor personnel accessing CHRI are either covered by the existing law or that the existing law is amended to include such Contractor personnel prior to authorizing outsourcing initiatives. The national criminal history record checks of Contractor personnel with access to CHRI cannot be outsourced and must be performed by the Authorized Recipient.

- occur and, if a criminal history record check is required, the Authorized Recipient shall maintain a list of Contractor personnel who successfully completed the criminal history record check.
- b. The Authorized Recipient shall ensure that the Contractor maintains site security. (See the current CJIS Security Policy [www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view])
 - c. The State Compact Officer/Chief Administrator or the FBI Compact Officer shall make available the most current versions of both the Outsourcing Standard and the CJIS Security Policy to the Authorized Recipient within 60 calendar days (unless otherwise directed) of notification of successor versions of the Outsourcing Standard and/or the CJIS Security Policy. The Authorized Recipient shall notify the Contractor within 60 calendar days of the FBI/state notification regarding changes or updates to the Outsourcing Standard and/or the CJIS Security Policy. The Authorized Recipient shall be responsible to ensure the most updated versions are incorporated by reference at the time of contract, contract renewal, or within the 60 calendar day notification period, whichever is sooner.
 - d. The Authorized Recipient and/or Contractor shall make available to the State Compact Officer/Chief Administrator or the FBI Compact Officer the relevant portions of the current and approved contract relating to CHRI, upon request.
- 2.04 The Authorized Recipient shall understand the communications and record capabilities of the Contractor which has access to federal or state records through, or because of, its outsourcing relationship with the Authorized Recipient. The Authorized Recipient shall request and approve a topological drawing which depicts the interconnectivity of the Contractor's network configuration as it relates to the outsourced function(s). The Authorized Recipient shall understand and approve any modifications to the Contractor's network configuration as it relates to the outsourced function(s). For approvals granted through the State Compact Officer/Chief Administrator, the Authorized Recipient, if required, shall coordinate the approvals with the State Compact Officer/Chief Administrator.
- 2.05 The Authorized Recipient is responsible for the actions of the Contractor and shall monitor the Contractor's compliance to the terms and conditions of the Outsourcing Standard. For approvals granted through the FBI Compact Officer, the Authorized Recipient shall certify to the FBI Compact Officer that an audit was conducted with the Contractor within 90 days of the date the Contractor first receives CHRI under the approved

outsourcing agreement. For approvals granted through the State Compact Officer/Chief Administrator, the Authorized Recipient, in conjunction with the State Compact Officer/Chief Administrator, will conduct an audit of the Contractor within 90 days of the date the Contractor first receives CHRI under the approved outsourcing agreement. The Authorized Recipient shall certify to the State Compact Officer/Chief Administrator that the audit was conducted.

- 2.06 The Authorized Recipient shall provide written notice of any early voluntary termination of the contract to the Compact Officer/Chief Administrator or the FBI Compact Officer.
- 2.07 The Authorized Recipient shall appoint an Information Security Officer. The Authorized Recipient's Information Security Officer shall:
 - a. Serve as the security POC for the FBI CJIS Division Information Security Officer.
 - b. Document technical compliance with this Outsourcing Standard.
 - c. Establish a security incident response and reporting procedure to discover, investigate, document, and report on major incidents that significantly endanger the security or integrity of the noncriminal justice agency systems to the CJIS Systems Officer, State Compact Officer/Chief Administrator and the FBI CJIS Division Information Security Officer.
- 2.08 The Authorized Recipient shall immediately (within one hour) notify the State Compact Officer/Chief Administrator or the FBI of any PII breach. The Authorized Recipient shall also provide a written report of any PII breach (to include unauthorized access to CHRI by the Contractor) to the State Compact Officer/Chief Administrator or the FBI within five calendar days of receipt of the initial report of the PII breach. The written report must include corrective actions taken by the Authorized Recipient and, if necessary, the Contractor to resolve such PII breach.

3.0 *Responsibilities of the Contractor*

- 3.01 The Contractor and its employees shall comply with all federal and state laws, regulations, and standards (including the CJIS Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.
- 3.02 The Contractor shall develop, document, administer, and maintain a Security Program (Physical, Personnel, and Information Technology) to comply with the most current Outsourcing Standard and the most current CJIS Security Policy. The Security Program shall describe the implementation of the security requirements outlined in this Outsourcing Standard and the CJIS Security Policy. In addition, the Contractor is also

responsible to set, maintain, and enforce the standards for the selection, supervision, and separation of personnel who have access to CHRI. The Authorized Recipient shall provide the written approval to the State Compact Officer/Chief Administrator or the FBI Compact Officer of a Contractor's Security Program. For approvals granted through the State Compact Officer/Chief Administrator, it is the responsibility of the State Compact Officer/Chief Administrator to ensure the Authorized Recipient is in compliance with the CJIS Security Policy.

- 3.03 The requirements for a Security Program should include, at a minimum:
- a) Description of the implementation of the security requirements described in this Outsourcing Standard and the CJIS Security Policy.
 - b) Security Training.
 - c) Guidelines for documentation of security violations to include:
 - i) Develop and maintain a written incident reporting plan to address security events, to include violations and incidents. (See the CJIS Security Policy {www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view}).
 - ii) A process in place for reporting security violations.
 - d) Standards for the selection, supervision, and separation of personnel with access to CHRI.
- **If the Contractor is using a corporate policy, it must meet the requirements outlined in this Outsourcing Standard and the CJIS Security Policy. If the corporate policy is not this specific, it must flow down to a level where the documentation supports these requirements.
- 3.04 Except when the training requirement is retained by the Authorized Recipient, the Contractor shall develop a Security Training Program for all Contractor personnel with access to CHRI prior to their appointment/assignment. The Authorized Recipient shall review and provide to the Contractor written approval of the Security Training Program. Training shall be provided upon receipt of notice from the Compact Officer/Chief Administrator on any changes to federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General. Annual refresher training shall also be provided. The Contractor shall annually, not later than the anniversary date of the contract, certify in writing to the Authorized Recipient that annual refresher training was completed for those Contractor personnel with access to CHRI.
- 3.05 The Contractor shall make its facilities available for announced and unannounced audits and security inspections performed by the Authorized Recipient, the state, or the FBI on behalf of the Compact Council.

- 3.06 The Contractor's Security Program is subject to review by the Authorized Recipient, the Compact Officer/Chief Administrator, and the FBI CJIS Division. During this review, provision will be made to update the Security Program to address security violations and to ensure changes in policies and standards as well as changes in federal and state law are incorporated.
 - 3.07 The Contractor shall maintain CHRI only for the period of time necessary to fulfill its contractual obligations but not to exceed the period of time that the Authorized Recipient is authorized to maintain and does maintain the CHRI.
 - 3.08 The Contractor shall maintain a log of any dissemination of CHRI, for a minimum of 365 days.
 - 3.09 The Authorized Recipient and/or Contractor shall make available to the State Compact Officer/Chief Administrator or the FBI Compact Officer the relevant portions of the current and approved contract relating to CHRI, upon request.
- 4.0 *Site Security*
- 4.01 The Authorized Recipient shall ensure that the Contractor site(s) is a physically secure location to protect against any unauthorized access to CHRI.
- 5.0 *Dissemination*
- 5.01 The Contractor shall not disseminate CHRI without the consent of the Authorized Recipient, and as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.
 - 5.02 An up-to-date log concerning dissemination of CHRI shall be maintained by the Contractor for a minimum one year retention period. This log must clearly identify: (A) the Authorized Recipient with unique identifiers to include the FBI assigned Originating Agency Identifiers to include the FBI assigned Originating Agency Identifier (ORI)/Originating Agency Case (OCA) number, (B) the Transaction Control Number (TCN), (C) the date of dissemination, (D) the statutory authority for dissemination, and (E) the means of dissemination.
 - 5.03 If CHRI is stored or disseminated in an electronic format, the Contractor shall protect against unauthorized access to the equipment and any of the data. In no event shall responses containing CHRI be disseminated other than as governed by this Outsourcing Standard or more stringent contract requirements.

6.0 *Personnel Security*

- 6.01 If a local, state, or federal written standard requires or authorizes a criminal history record check of the Authorized Recipient's personnel with access to CHRI, then a criminal history record check shall be required of the Contractor's (and approved Sub-Contractor's) employees having access to CHRI. Criminal history record checks of Contractor and approved Sub-Contractor employees, at a minimum, will be no less stringent than criminal history record checks that are performed on the Authorized Recipient's personnel performing similar functions. Criminal history record checks must be completed prior to accessing CHRI under the contract.
- 6.02 The Contractor shall ensure that each employee performing work under the contract is aware of the requirements of the Outsourcing Standard and the state and federal laws governing the security and integrity of CHRI. The Contractor shall confirm in writing that each employee has certified in writing that he/she understands the Outsourcing Standard requirements and laws that apply to his/her responsibilities. The Contractor shall maintain the employee certifications in a file that is subject to review during audits. Employees shall make such certification prior to performing work under the contract.
- 6.03 The Contractor shall maintain updated records of personnel who have access to CHRI, update those records within 24 hours when changes to that access occur, and if a criminal history record check is required, maintain a list of personnel who have successfully completed criminal history record checks. The Contractor shall notify Authorized Recipients within 24 hours when additions or deletions occur.

7.0 *System Security*

- 7.01 The Contractor's security system shall comply with the CJIS Security Policy in effect at the time the Outsourcing Standard is incorporated into the contract and with successor versions of the CJIS Security Policy.
- a. Devices shall be implemented to provide a point of defense and a controlled and audited access to CHRI, both from inside and outside the networks.
 - b. Data encryption shall be required for data in transit pursuant to the requirements in the CJIS Security Policy.
- 7.02 The Contractor shall provide for the secure storage and disposal of all hard copy and media associated with the system to prevent access by unauthorized personnel.
See the current CJIS Security Policy to address:

[www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view]

- a. Physically secure location.
 - b. Sanitization procedures for all fixed and non-fixed storage media.
 - c. Storage procedures for all fixed and non-fixed storage media.
- 7.03 To prevent and/or detect unauthorized access to CHRI in transmission or storage, each Authorized Recipient, Contractor, or Sub-Contractor must be assigned a unique identifying number.

8.0 *Security Violations*

8.01 Duties of the Authorized Recipient and Contractor

- a. The Authorized Recipient shall develop and maintain a written policy for discipline of Contractor employees who violate the security provisions of the contract, which includes this Outsourcing Standard that is incorporated by reference. The Authorized Recipient shall develop and maintain a written incident reporting plan for security events, to include violations and incidents. (See also Sections 2.07 and 3.03)
- b. Pending investigation, the Contractor shall, upon detection or awareness, suspend any employee who commits a security violation from assignments in which he/she has access to CHRI under the contract.
- c. The Contractor shall immediately (within one hour of discovery) notify the Authorized Recipient, the State Compact Officer/Chief Administrator, or the FBI of any security violation to include unauthorized access to CHRI. Within five calendar days of such discovery, the Contractor shall provide the Authorized Recipient, the State Compact Officer/Chief Administrator or the FBI a written report documenting such security violation, corrective actions taken by the Contractor to resolve such violation, and the date, time, and summary of the violation.
- d. The Authorized Recipient shall immediately (within four hours) notify the State Compact Officer/Chief Administrator and the FBI Compact Officer of any security violation or termination of the contract, to include unauthorized access to CHRI made available pursuant to the contract. The Authorized Recipient shall provide a written report of any security violation (to include unauthorized access to CHRI by the Contractor) to the State Compact Officer/Chief Administrator, if applicable, and the FBI Compact Officer, within five calendar days of receipt of the written report from the Contractor. The written report must include any corrective actions taken by the Contractor and the Authorized Recipient to

resolve such security violation.

- 8.02 Termination of the contract by the Authorized Recipient for security violations
 - a. The contract is subject to termination by the Authorized Recipient for security violations involving CHRI obtained pursuant to the contract.
 - b. The contract is subject to termination by the Authorized Recipient for the Contractor's failure to notify the Authorized Recipient of any security violation or to provide a written report concerning such violation.
 - c. If the Contractor refuses to or is incapable of taking corrective actions to successfully resolve a security violation, the Authorized Recipient shall terminate the contract.
- 8.03 Suspension or termination of the exchange of CHRI for security violations
 - a. Notwithstanding the actions taken by the State Compact Officer, if the Authorized Recipient fails to provide a written report notifying the State Compact Officer/Chief Administrator or the FBI Compact Officer of a security violation, or refuses to or is incapable of taking corrective action to successfully resolve a security violation, the Compact Council or the United States Attorney General may suspend or terminate the exchange of CHRI with the Authorized Recipient pursuant to 28 CFR §906.2(d).
 - b. If the exchange of CHRI is suspended, it may be reinstated after satisfactory written assurances have been provided to the Compact Council Chairman or the United States Attorney General by the Compact Officer/Chief Administrator, the Authorized Recipient and the Contractor that the security violation has been resolved. If the exchange of CHRI is terminated, the Contractor's records (including media) containing CHRI shall be deleted or returned in accordance with the provisions and time frame as specified by the Authorized Recipient.
- 8.04 The Authorized Recipient and Contractor shall provide written notice (through the State Compact Officer/Chief Administrator if applicable) to the FBI Compact Officer of the following:
 - a. The termination of a contract for security violations.
 - b. Security violations involving the unauthorized access to CHRI.
 - c. The Contractor's name and unique identification number, the nature of the security violation, whether the violation was intentional, and the number of times the violation occurred.
- 8.05 The Compact Officer/Chief Administrator, Compact Council and the

United States Attorney General reserve the right to investigate or decline to investigate any report of unauthorized access to CHRI.

- 8.06 The Compact Officer/Chief Administrator, Compact Council, and the United States Attorney General reserve the right to audit the Authorized Recipient and the Contractor's operations and procedures at scheduled or unscheduled times. The Compact Council, the United States Attorney General, and the state are authorized to perform a final audit of the Contractor's systems after termination of the contract.

9.0 *PII*

- 9.01 The Contractor is responsible for protecting all PII in its possession and control when handling, using, or storing CHRI.
- 9.02 The Contractor shall notify authorized individuals of their right to report PII breaches directly to the FBI should they believe their information has been mishandled or compromised.
- 9.03 The Contractor shall immediately (within one hour of discovery) notify the Authorized Recipient, the State Compact Officer/Chief Administrator, or the FBI of any PII breach or potential PII breach. Within five calendar days of such discovery, the Contractor shall provide the Authorized Recipient, the State Compact Officer/Chief Administrator, or the FBI a written report documenting such violation and corrective actions taken to resolve such violation, to include the date, time, and summary of the notification to resolve such breach.

10.0 *Miscellaneous Provisions*

- 10.01 This Outsourcing Standard does not confer, grant, or authorize any rights, privileges, or obligations to any persons other than the Contractor, the Authorized Recipient, Compact Officer/Chief Administrator (where applicable), and the FBI.
- 10.02 The following document is incorporated by reference and made part of this Outsourcing Standard: (1) The CJIS Security Policy.
- 10.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they provide a minimum basis for the security of the system and the CHRI accessed therefrom and it is understood that there may be terms and conditions of the appended contract which impose more stringent requirements upon the Contractor.⁵

⁵Such conditions could include additional audits, fees, or security requirements. The Compact Council, Authorized Recipients, and the Compact Officer/Chief Administrator have the explicit authority to require more stringent standards than those contained in the Outsourcing Standard.

- 10.04 The minimum security measures as outlined in this Outsourcing Standard may only be modified by the Compact Council. Conformance to such security measures may not be less stringent than stated in this Outsourcing Standard without the consent of the Compact Council in consultation with the United States Attorney General.
- 10.05 This Outsourcing Standard may only be modified by the Compact Council and may not be modified by the parties to the appended contract without the consent of the Compact Council.
- 10.06 Appropriate notices, assurances, and correspondence to the FBI Compact Officer, Compact Council, and the United States Attorney General required by Section 8.0 of this Outsourcing Standard shall be forwarded by First Class Mail to:
- FBI Compact Officer
1000 Custer Hollow Road
Module D-3
Clarksburg, WV 26306

11.0 *Exemption from Above Provisions*

11.01 An Information Technology (IT) contract need only include Sections 1.0, 2.01, 2.02, 2.03, 3.01, 6.0, 8.0, and 9.0 of this Outsourcing Standard for Non-Channelers when all of the following conditions exist:

1. Access to CHRI by the IT contractor's personnel is limited solely for the development and/or maintenance of the Authorized Recipient's computer system;
2. Access to CHRI is incidental, but necessary, to the duties being performed by the IT contractor;
3. The computer system resides within the Authorized Recipient's facility;
4. The Authorized Recipient's personnel supervise or work directly with the IT contractor personnel;
5. The Authorized Recipient maintains complete, positive control of the IT contractor's access to the computer system and CHRI contained therein; and
6. The Authorized Recipient retains all of the duties and responsibilities for the performance of its authorized noncriminal justice administrative functions, unless it executes a separate contract to perform such noncriminal justice administrative functions, subject to all applicable requirements, including the Outsourcing Standard.

11.02 An Authorized Recipient's contract where access to CHRI is limited solely

for the purposes of: (A) storage (referred to as archiving in some states) of the CHRI at the Contractor's facility; (B) retrieval of the CHRI by Contractor personnel on behalf of the Authorized Recipient with appropriate security measures in place to protect the CHRI; and/or (C) destruction of the CHRI by Contractor personnel when not observed by the Authorized Recipient need only include Sections 1.0, 2.01, 2.02, 2.03, 3.01, 4.0, 6.0, 8.0, and 9.0 of this Outsourcing Standard for Non-Channelers when all of the following conditions exist:

1. Access to CHRI by the Contractor is limited solely for the purposes of: (A) storage (referred to as archiving in some states) of the CHRI at the Contractor's facility; (B) retrieval of the CHRI by Contractor personnel on behalf of the Authorized Recipient with appropriate security measures in place to protect the CHRI; and/or (C) destruction of the CHRI by Contractor personnel when not observed by the Authorized Recipient;
2. Access to CHRI is incidental, but necessary, to the duties being performed by the Contractor;
3. The Contractor is not authorized to disseminate CHRI to any other agency or contractor on behalf of the Authorized Recipient;
4. The Contractor's personnel are subject to the same criminal history record checks as the Authorized Recipient's personnel;
5. The criminal history record checks of the Contractor personnel are completed prior to work on the contract or agreement;
6. The Authorized Recipient retains all other duties and responsibilities for the performance of its authorized noncriminal justice administrative functions, unless it executes a separate contract to perform such noncriminal justice administrative functions, subject to all applicable requirements, including the Outsourcing Standard; and
7. The Contractor stores the CHRI in a physically secure location.

12.0 *Duties of the State Compact Officer/Chief Administrator*

12.01 The State Compact Officer/Chief Administrator shall review legal authority and respond in writing to the Authorized Recipient's request to outsource noncriminal justice administrative functions.

- 12.02 The State Compact Officer/Chief Administrator reserves the right to review relevant portions of the outsourcing contract relating to CHRI throughout the duration of the contract approval.
- 12.03 The State Compact Officer/Chief Administrator must ensure criminal history record checks on approved Contractor and Sub-Contractor employees with access to CHRI are completed by the Authorized Recipient, if such checks are required or authorized of the Authorized Recipient personnel by federal statute, executive order, or state statute approved by the United States Attorney General under Public Law 92-544. Criminal history record checks should be no less stringent than the checks performed on the Authorized Recipient personnel. Criminal history record checks must be completed prior to accessing CHRI under the contract.
- 12.04 Coordinate with the Authorized Recipient for the review and approval of the Contractor's Topological drawing which depicts the interconnectivity of the Contractor's network configuration as it relates to the outsourcing function(s).
- 12.05 90 Day Compliance Review
- a. The State Compact Officer/Chief Administrator shall work in coordination with the Authorized Recipient to conduct an audit of the Contractor within 90 days of the date the Contractor first receives CHRI under the approved outsourcing agreement.
 - b. The State Compact Officer/Chief Administrator shall review the Authorized Recipient's audit certification to ensure compliance with the Outsourcing Standard.
 - i) The State Compact Officer/Chief Administrator shall address concerns with the Authorized Recipient resulting in non-compliance with the 90 day audit of the Contractor.
 - ii) The State Compact Officer/Chief Administrator shall have the right to terminate an Authorized Recipient's Outsourcing approval to a Contractor(s) for failure or refusal to correct a non-compliance issue(s).
- 12.06 The State Compact Officer/Chief Administrator shall coordinate with the Authorized Recipient to review the Contractor's Security Program. The program shall describe the implementation of the security requirements outlined in this Outsourcing Standard and the CJIS Security Policy. During the review, provisions will be made to update the Security Program to address security events and to ensure changes in policies and standards, as well as changes in federal and state law, are incorporated.
- 12.07 The State Compact Officer/Chief Administrator shall audit the Authorized Recipient and/or Contractor's operations and procedures. This may be done at scheduled and unscheduled times.
- 12.08 The State Compact Officer/Chief Administrator shall assign a unique

identifying number to each Authorized Recipient, Contractor, or Sub-Contractor to ensure system security.

- 12.09 The State Compact Officer/Chief Administrator shall require immediate (within four hours) notification by the Authorized Recipient of any security event, to include security violations and incidents or termination of the contract, to include unauthorized access to CHRI made available pursuant to the contract. The State Compact Officer/Chief Administrator shall receive a written report from the Authorized Recipient of any security event (to include unauthorized access to CHRI by the Contractor) within five calendar days of receipt of the written report from the Contractor, that must include any corrective actions taken by the Contractor and Authorized Recipient to resolve such security event. (See the CJIS Security Policy {www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view})
- 12.10 Suspension or termination of the exchange of CHRI for security events.
 - a. The State Compact Officer/Chief Administrator may suspend or terminate the exchange of CHRI for security events or refusal or incapability to take corrective action to successfully resolve a security event.
 - b. The State Compact Officer/Chief Administrator may reinstate access to CHRI between the Authorized Recipient and the Contractor after receiving written assurance(s) of corrective action(s) from the Authorized Recipient and/or the Contractor.
- 12.11 The State Compact Officer/Chief Administrator shall provide written notification to the FBI Compact Officer of the termination of a contract for security events to include the security events involving access to CHRI; the Contractor's name and unique identification number; the nature of the security event; whether the event was intentional; and the number of times the event occurred.
- 12.12 The State Compact Officer/Chief Administrator reserves the right to investigate or decline to investigate any report of unauthorized access to CHRI.
- 12.13 The State Compact Officer/Chief Administrator is authorized to perform a final audit of the Contractor's system following termination of contract.

Clarification on Submission of Outsourcing Agreements

On February 13, 2020, during the Oklahoma City Regional Training Course, TGRAs requested clarification for when TGRAs are required to request FBI Compact Officer approval to outsource non-criminal justice administrative functions with a non-channeler. Specifically, when does escorting a contractor and encryption of electronic Criminal History Record Information (CHRI) remove the need to request FBI Compact Officer approval?

As a result of these questions, NIGC contacted the FBI Compact Officer for clarification. The FBI Compact Officer clarified that fully escorting, such as in the case with document shredders, and encrypting CHRI, such as in the case with IT service contracts, do not relieve the requirement to request FBI Compact Officer approval for contractors accessing CHRI.

However, if the contractor is fully escorted and if the contractor is providing limited IT services, some of the Security and Management Control Outsourcing Standard for Non-Channelers as identified in Sections 11.01 and 11.02 of that document are exempted. There are several conditions listed in both Section 11.01 and 11.02 that must be met to exempt these provisions within the Standard. However, even when all conditions are met, Section 2.01 - requiring FBI Compact Officer approval - remains a relevant portion of the Standard that must be incorporated into the contract. As such, outsourcing (e.g., IT services, shredding) that falls within these areas, must be formally approved by the FBI Compact Officer.

The effect of this clarification is TGRAs must submit request letters to the FBI Compact Officer for all contractors with physical or logical access to their CHRI for the purpose of conducting a non-criminal justice administrative function¹, regardless if they will be fully escorted or the steps that have been taken to secure the CHRI, such as encryption.

This clarification will result in the current NIGC CJIS Manual and training material being updated for the next RTC and future training sessions. TGRA are encouraged to continue to identify all contractors currently engaged for these administrative functions; prepare and submit request letters and copies of all proposed outsourcing agreements with such contractors to the FBI Compact Officer for approval, copying the NIGC ISO (iso@nigc.gov); and complete the required 90-day audit and required certification.

Both the FBI Compact Officer and CJIS Audit staff have informed NIGC that the desire to simplify and unify the outsourcing requirements for non-channelers, channeler, non-criminal justice agencies and criminal justice agencies under the CJIS Security Policy and Outsourcing Standards has led them to propose changes this year to the committee that drafts policy revisions for Compact Council approval. They anticipate changes may be accepted for review and implementation starting in November of 2020. NIGC will update all parties should any changes be accepted and adopted by the Compact Council affecting how NIGC and TGRAs identify and process requests for outsourcing non-criminal justice administrative functions with non-channelers and any new exemptions.

We have included a link here to the current version (2018) of the Security and Management Control Outsourcing Standard for Non-Channelers for your reference and review: <https://www.fbi.gov/file-repository/compact-council-security-and-management-control-outsourcing-standard-for-non-channelers.pdf/view>

Links to sample request letters and sample contracts for FBI Compact Officer approval can be found in the Outsourcing Agreements section on this page: <https://www.nigc.gov/compliance/CJIS-Training-Materials>

NIGC will continue to assist TGRAs in the implementation of the CJIS Security Policy and other related standard. We welcome your questions about the policy and continued feedback about the implementation process.

¹ Noncriminal Justice Administrative Functions means the routine noncriminal justice administrative functions relating to the processing of CHRI, including but not limited to: 1. Making fitness determinations/recommendations; 2. Obtaining missing dispositions; 3. Disseminating CHRI as authorized by Federal statute, Federal Executive Order, or State statute approved by the United States Attorney General; and 4. Other authorized activities relating to the general handling, use, and storage of CHRI.



National Identity Services Audit

Noncriminal Justice Access to Criminal History Record Information

Policy Reference Guide



Telephone – 304-625-3020
E-mail – <NISAudit@leo.gov>

Table of Contents

Criminal History Record Information	1
Use of CHRI	2
Fingerprint-based	
Coordination and Approval	
Authorized Requests	
Implementation	
Re-use	
Name-based	
Coordination and Approval	
Authorized Requests	
Implementation	
Re-use	
Dissemination of CHRI	5
Authorized Recipients	
Receiving Departments	
Related Agencies	
Single Need/Purpose	
Multiple Needs/Purposes	
Other Authorized Entities	
Jurisdictional Control	
Public Access	
Additional Considerations	
General	
Notifications	
Subject of the Record	
Residual Access	
Purpose for Disclosure of CHRI	11
Reason Fingerprinted Field	
Interstate Identification Index Purpose Codes	
Reason for Request	
Agency Identifiers for Receipt of CHRI	
Independent Application, Fingerprinting, and Adjudication Processes	
Documentation of Reason for Request	
Applicant Notification and Record Challenge	12
Privacy Act Statement	
Opportunity to Complete or Challenge a Record	
Procedures for Obtaining a Record Change	
Additional Considerations	
Noncriminal Justice Agency Audits	14
User Fee	15
Criminal Justice (No-fee)	
Volunteer (Reduced-fee)	
Abbreviations and Acronyms	16

Criminal History Record Information

The Compact, at Title 34, U.S.C., Section 40316, Article I, includes the same statutory definition of CHRI as that established at Title 28, CFR, Section 20.3: information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, and release; the term does not include identification information such as fingerprint records if such information does not indicate the individual's involvement with the criminal justice system. In addition, the *CJIS Security Policy* defines CHRI as a subset of Criminal Justice Information consisting of any notations or other written or electronic evidence of an arrest, detention, complaint, indictment, information, or other formal criminal charge relating to an identifiable person that includes identifying information regarding the individual as well as the disposition of any charges.

Information is considered CHRI if it is transferred or reproduced directly from CHRI received as a result of a national FBI check and associated with the subject of the record. This includes information such as conviction/disposition data as well as identifiers used to index records regardless of format. Examples of formal and informal products or verbalizations include: correspondence such as letters and e-mails; documents such as forms and hand-written notes; conversations either in person or by telephone; and data fields such as those stored in database tables or spreadsheets. However, information is not considered CHRI if it is obtained as a result of using CHRI received from a national FBI check as a lead to reach out to source record owners such as local courts or state criminal history record repositories. As a prerequisite, both the process used to obtain the source record information and the resulting source record information itself must not directly reference or be attributed to the national FBI check.

Information is considered CHRI if it confirms the existence or nonexistence of CHRI. This FBI policy is derived from and mirrors the general policy on dissemination found at Title 28, CFR, Section 20.21, directly relating to applicable state and local criminal history record information systems. This includes applicant status information, which is either directly attributed to or predominately based on a national FBI check, when no recognized authority or inherent need exists for the release of such information.

Use of CHRI

The requirements for the use of CHRI for noncriminal justice purposes are derived from various federal statutes, regulations, policies, and interpretations thereof, to include rules and procedures promulgated by the Compact Council. Primary references for these requirements include:

- Title 28, U.S.C., Section 534 (a)(4)
- Title 34, U.S.C., Section 40316, Article IV (c) and Article V (a) and (c)
- Title 28, CFR, Section 20.33
- Title 28, CFR, Section 50.12
- Title 28, CFR, Section 901
- *III/NFF Operational and Technical Manual*, Chapter 3
- CJIS Advisory Policy Board, *Concept for the Exchange of Criminal History Records for Noncriminal Justice Uses by Means of The III*, Section B
- Compact Council's Noncriminal Justice Online Policy Resources

The NIS audit assesses four categories of requirements associated with the use of CHRI for noncriminal justice purposes: (1) Authorized Requests, (2) Implementation, and (3) Re-use. While baseline requirements for both fingerprint-based and name-based use of CHRI for noncriminal justice purposes essentially parallel one another, the four categories of requirements are presented from both perspectives for clarity and reporting purposes.

Use of CHRI (Fingerprint-based)

Unless authorized pursuant to federal statutory authority or Compact Council regulations promulgated based upon federal statutory authority, noncriminal justice background checks of the III System must be supported by fingerprints or other approved forms of positive identification in order to determine that the subject of a record search is the same person as the subject of a criminal history record indexed in the III System. This requirement is memorialized in the Compact. The Compact Council has accepted two methods for determining positive identification for exchanging CHRI for noncriminal justice purposes, ten-rolled fingerprints and ten-flat fingerprints.

Coordination and Approval

Agencies must only leverage recognized/approved authorities for submission of noncriminal justice fingerprint-based requests for CHRI. Examples of such authorities include Public Law 92-544, the NCPA/VCA, the Adam Walsh Act, and the Serve America Act. Prior to implementation of any federal statutory authority, a state or federal agency must coordinate with the FBI to determine the requirements for submitting under the specific authority (e.g., system changes, issuance of an ORI, fingerprint submission procedures, use of specific reason fingerprinted, etc.), and when applicable, obtain formal approval prior to use. When applicable, agencies must also obtain updated approval from the FBI for any changes associated with a previously approved authority, such as Public Law 92-544 state statutes. In addition, agencies must notify the FBI which authority is the exclusive remedy when multiple approved authorities exist for a particular purpose (applicant type). This specific requirement currently applies when states must formally designate either an approved Public Law 92-544 state statute or the NCPA/VCA for providers of care to vulnerable populations if state law is not clear or silent on the NCPA/VCA.

Authorized Requests

Agencies must only submit noncriminal justice fingerprint-based requests for CHRI for purposes (applicant types) covered by the authority leveraged for the request. In addition, agencies must only submit requests for purposes that are known to exist at the time of submission. Agencies must not submit requests for a future anticipated need, even if the need is covered by an approved authority.

Implementation

Agencies must implement all applicable administrative and procedural provisions associated with the authority leveraged to submit noncriminal justice fingerprint-based requests for CHRI (e.g., signed applicant statements under NCPA/VCA and VECHS agency user agreements).

Re-use

Agencies must only use CHRI received as a result of noncriminal justice fingerprint-based requests for the specific purpose originally requested. Agencies must not subsequently re-use CHRI for unrelated needs, even if the new needs are covered by a recognized/approved authority. A purpose or need for use is a request for CHRI to adjudicate a specific application for a noncriminal justice purpose (e.g., license, position of employment, benefit, etc.) that is known at the time the request is made, pursuant to an approved statutory authority, and based on the positive identification via fingerprint submission of the applicant. The basic parameters for use consists of (chronologically): 1) authority for access, 2) application and fingerprint submission, 3) receipt of CHRI, 4) adjudication, and 5) closing or maintenance activities.

However, if a special set of circumstances exist that show an extremely close relation to the original purpose, CHRI that was made available for the original purpose could possibly be used again for the new purpose. Under this premise, the new purpose is so closely related to the original purpose that both are considered singular in nature. The primary factors when considering the circumstances that may potentially relate multiple purposes include: the statutory authority being used; the agency or agencies involved; the type of license/position of employment/benefit being applied for; and the application/adjudication process. This consideration is based on standing audit practices and legal interpretations of related agency as applied to the use of CHRI. It is important to note that this type of acceptable re-use is quite infrequent and very dependent upon the specific scenario involved. As such, it is highly recommended that re-use of this nature be closely coordinated with the FBI prior to implementation. For example, a person applies to be a substitute teacher with public School Board A. School Board A completes the fingerprint process and submits the fingerprints pursuant to an approved state statute that authorizes background checks for school employment purposes. Then one month later the individual also applies to be a substitute teacher with public School Board B. School Board B requests a copy of the CHRI from School Board A which provides it. In this case, since School Board A and School Board B are both covered by the same statute and using CHRI for a similar applicant type within a relatively short period of time, these can be considered to be for the same purpose. However, if the applicant had applied one month later for a liquor license from the ABC Board, School Board A would not be permitted to provide the CHRI to the ABC Board. Although the background checks are in a relatively short period of time of each other, the applicant types are significantly

different enough, and the ABC Board would not be covered by the same statutory authority as School Board A. In addition, CHRI may be re-used in limited circumstances under the NCPA/VCA VECHS program.

It is important to note that FBI CHRI is considered instantly outdated as new information may be added to the record or deleted at any time. Although re-use of CHRI in certain situations may be acceptable, agencies that accept the risk of using outdated CHRI must understand that the information is subject to change.

Use of CHRI (Name-Based)

Access to the III System using name-based queries and record request messages is not permitted for noncriminal justice purposes, unless authorized pursuant to federal statutory authority or Compact Council regulations promulgated based upon federal statutory authority.

Coordination and Approval

Agencies must only leverage recognized/approved authorities for submission of name-based noncriminal justice III System queries and record request messages. Examples of such authorities include the Compact Council's Fingerprint Submission Requirements Rule (Purpose Code X), the Housing Opportunity Extension Act (Purpose Code H), and the Security Clearance Information Act (Purpose Code S). When applicable, agencies must coordinate with the FBI to determine specific requirements for use of a particular authority and obtain formal approval prior to use (e.g., Purpose Code X). When applicable, agencies must also obtain updated approval from the FBI for any changes associated with a previously approved authority.

Authorized Requests

Agencies must only submit name-based noncriminal justice III System queries and record request messages for authorized purposes covered by the authority leveraged for the request (i.e., federal statutory authority or Compact Council regulations promulgated based upon federal statutory authority). In addition, agencies must only submit requests for purposes that are known to exist at the time of submission. Agencies must not submit requests for a future anticipated need, even if the need is covered by an approved authority.

Implementation

Agencies must implement applicable administrative/procedural provisions required by the authority leveraged to submit name-based III checks for noncriminal justice purposes (e.g., follow-up fingerprints for Purpose Code X and limits on direct access by public housing authorities for Purpose Code H).

Re-use

Agencies must only use CHRI received as a result of noncriminal justice name-based III System queries and record request messages for the specific purpose originally requested. Agencies must not subsequently re-use CHRI for unrelated needs, even if the new needs are covered by a recognized/approved authority. Congruent with requirements for CHRI received as a result of fingerprint-based requests, re-use of CHRI received via name-based III checks may be acceptable in limited circumstances.

Dissemination of CHRI

The requirements for the dissemination of CHRI for noncriminal justice purposes are derived from various federal statutes, regulations, policies, and interpretations thereof, to include rules and procedures promulgated by the Compact Council. Primary references for these requirements include:

- Title 28, U.S.C., Section 534 (a)(4)
- Title 34, U.S.C., Section 40316, Article IV (c)
- Title 28, CFR, Section 20.33
- Title 28, CFR, Section 50.12
- Title 28, CFR, Section 906
- *III/NFF Operational and Technical Manual*, Chapter 3
- Compact Council's Noncriminal Justice Online Policy Resources

The NIS audit assesses three categories of requirements for dissemination of CHRI for noncriminal justice purposes: (1) Authorized Recipients, (2) Jurisdictional Control, and (3) Public Access. These categories center on the baseline requirement for allowable dissemination to receiving departments, related agencies, and other authorized entities. It should be noted that while the requirements below are written primarily from a state perspective, they also apply to federal and federally-regulated agencies that request, receive, and use CHRI for noncriminal justice purposes.

Authorized Recipients (Receiving Departments and Related Agencies)

CHRI may only be disseminated to receiving departments and related agencies that are authorized relative to the federal statutory authority used to obtain CHRI. States must ensure that recipients fall within allowable parameters established by federal statutory authorities leveraged for national criminal history checks.

As with the use of CHRI, parameters for dissemination are derived from the specific federal statutory authority leveraged to obtain CHRI. CHRI may only be disseminated to entities that are authorized relative to the federal statutory authority used to submit a fingerprint check. For example:

- Dissemination is limited to officials of state and local governments for CHRI obtained pursuant to Public Law 92-544.
- Dissemination is limited to "authorized agencies" defined as a division or office of a state for CHRI obtained pursuant to the NCPA/VCA. However, dissemination of CHRI is extended to nongovernmental qualified entities if a VECHS program is implemented.
- Dissemination is limited to the following entities for CHRI obtained pursuant to the Adam Walsh Act: 1) child welfare agencies, which include states, local agencies, other public agencies, or any other private agencies under contract with a state or local agency responsible for licensing or approval of foster or adoptive parents; and 2) public or private elementary or secondary schools as well as state and local educational agencies.
- Dissemination is limited to governmental agencies for CHRI obtained pursuant to the Serve America Act.

It is important to recognize that state or local laws, ordinances, administrative rules, or procedures may not be more permissive regarding dissemination of CHRI relative to the federal

authority used to obtain CHRI. However, states may be more restrictive and establish additional limitations on dissemination.

Receiving Departments

States should designate primary authorized recipients responsible for accessing or receiving CHRI directly from the state repository for noncriminal justice purposes. These agencies typically have statutory authority or regulatory obligations associated with making fitness determinations and/or providing oversight of the employment or licensing processes for particular categories of applicants. States must ensure that primary receiving agencies fall within parameters established by the federal statutory authorities being leveraged for national criminal history checks. CHRI may only be disseminated to entities that are authorized relative to the federal statutory authority used to obtain CHRI.

Depending upon the specific procedures used by a state, there may be multiple primary agency types with access to CHRI for a particular type of national criminal history check. For example, while one state's procedures may only include disseminating CHRI directly to a Department of Education for background checks of teachers, another state's procedures may include dissemination of CHRI directly to each local county school board. Still another state's procedures may include simultaneously disseminating CHRI directly to both the Department of Education and a local county school board.

The term "agency" encompasses offices, departments, bureaus, and other subdivisions associated with a particular agency's organizational structure. Although baseline dissemination requirements for CHRI are centered at the department and agency levels, as a best business practice, states should limit access to the minimum necessary sub-offices and personnel within a department or agency that are actually required for a particular use. While authorized receiving agencies may exercise some level of discretion and freedom of maneuver to distribute CHRI within their organizational structure, they should be able to demonstrate a reasonable need for doing so. For example, a local county school board may be designated as an authorized recipient of CHRI for the purpose of conducting background checks for prospective teachers. CHRI is stored as part of an electronic personnel records management system accessible by all school board employees. Although the school board is an authorized recipient, it is in the agency's best interests to limit access to CHRI on the system to only the personnel within the human resources department responsible for making fitness determinations. This will limit the school board's exposure to the inherent risks associated with unauthorized dissemination of CHRI.

Many statutory authorities leveraged for national criminal history record checks limit dissemination to governmental agencies. Most governmental agencies are readily identified, such as those statutorily designated, funded, and organized as part of a state's executive, legislative, and judicial branches. However, governmental entities, such as commissions and boards that may be comprised of political appointees, elected officials, and/or officials from private industry, may also qualify as authorized recipients of CHRI. Examples could include school boards and lottery commissions.

Related Agencies

Two primary categories of related agency exist with respect to dissemination of CHRI. The categories are based on the use of CHRI for a single need versus multiple needs, and are derived from historical definitions of related agency doctrine as well as standing audit practices and legal interpretations.

- *Dissemination of CHRI to related agencies for a single need/purpose.* This type of dissemination of CHRI occurs when multiple agencies are involved in making a single fitness determination associated with an application for a specific authorized noncriminal justice purpose, such as a license, position of employment, or benefit. In many instances, this type of related agency is a secondary recipient of CHRI from a primary agency that receives CHRI directly from the state level. The intent is to allow some level of flexibility within the allowable parameters established by the federal statutory authority being leveraged for the national criminal history check. For example, with the state's consent, the Department of Education and local county school boards are both involved in adjudication of teacher employment applications. In addition, on an ad-hoc basis, some of these local county school boards make CHRI available to their local Sheriff's Office in order to answer questions regarding specific charges on criminal history records. Another example includes, with the state's consent, the Bureau of Professional Licensing and the Real Estate Commission are both involved in adjudication of real estate license applications.
- *Dissemination of CHRI to related agencies for multiple needs/purposes.* This type of dissemination of CHRI occurs when multiple agencies are involved in making fitness determinations for separate but related needs associated with multiple applications for specific authorized noncriminal justice purposes, such as a license, position of employment, or benefit. This type of dissemination directly correlates to the re-use of CHRI for related needs as described in the Compact Council's online policy resource, *Use of FBI CHRI for Noncriminal Justice Purposes*. For example, if established requirements are met, there are limited instances when CHRI may be disseminated between agencies pursuant to the Public Law 92-544 Article IV sharing initiative or the NCPA/VCA VECHS program. However, just as CHRI must not be re-used for subsequent unrelated needs by the original requestor/recipient, it is imperative to recognize that CHRI must also not be disseminated to another recipient for subsequent unrelated re-use. In addition, CHRI may not be disseminated to another recipient for future anticipated uses, regardless of whether or not the needs are formally related.

Just as with the primary receiving agency, any related secondary recipient must also be authorized relative to the federal statutory authority used to obtain CHRI. For example, agencies related for the purpose of adjudicating an employment application for child day care pursuant to Public Law 92-544 must be governmental. Note that even though a private employer, such as a day care center, may be perceived as having a commonality of purpose, CHRI may not be disseminated to them by the governmental agency. States should be able to demonstrate a reasonable need for which they have designated agencies as related for the purpose of adjudicating a particular type of applicant.

It is important to recognize the distinction between authorized recipients, related agencies, and contractors. A related agency is essentially a specially designated authorized recipient with an inherent authority to access CHRI, and therefore does not require formal implementation of the Compact Council's *Security and Management Control Outsourcing Standard for Non-Channelers*. However, a governmental or private contractor has no such inherent authority, and therefore does require formal outsourcing implementation. Authorized recipients may not leverage outsourcing to create an authority for the intended purpose of designating an entity as a related agency. For example, pursuant to Public Law 92-544, local county school boards are typically considered to be related to the Department of Education; however, private schools would not be considered related agencies, because they are nongovernmental. As such, the Department of Education could not implement outsourcing to designate a private school as a "contractor" to allow the private school access to CHRI for the purpose of making fitness determinations on the private school's applicants. As an alternative, the state could consider leveraging the Adam Walsh Act or the NCPA/VCA VECHS program, both of which authorize dissemination to nongovernmental entities, thus designating such entities as authorized recipients.

Other Authorized Entities

For NIS audit purposes, other authorized entities represent assessments of specific requirements not directly assessed or reported as part of the Authorized Recipients category.

Jurisdictional Control

Agencies outside of a state's jurisdiction cannot be designated as related agencies, even when a congruent related need appears to exist for the use of CHRI. The dissemination restriction primarily centers on each state's individual authority and obligation to administer access to CHRI. Each state has the authority to determine whether or not to conduct particular types of noncriminal justice background checks, and each state is responsible for establishing the mechanisms and procedures for those checks within its jurisdiction. In addition, each state possess limited authority to meet obligations for maintaining appropriate controls, such as user agreements and audits, outside of its jurisdiction, especially with respect to another state's governmental agencies. In conjunction with the more obvious jurisdictional concerns associated with one state's governmental agency leveraging another state's statutes under Public Law 92-544, similar jurisdictional concerns also exist with the use of other statutory authorities such as the Adam Walsh Act or the NCPA/VCA. Examples of unauthorized dissemination include:

- One state governmental agency sharing CHRI with another state's governmental agency for adoption purposes when the child and prospective parents reside in different states, even if both states have approved Public Law 92-544 state statutes.
- Criminal history sharing initiatives involving participation in national compacts, associations, or databases such as those for child placement or employment/licensing in the health care industry.

This dissemination restriction is not intended to limit a state from making CHRI available in very limited situations to certain nongovernmental entities outside of the state's geographical boundaries when such dissemination is specifically authorized and formal jurisdictional authority is established to maintain adequate controls. It is very important to recognize that in order for dissemination to occur beyond a state's geographical

boundaries, there must first be an approved statutory authority which allows nongovernmental entities access to CHRI within the state's geographical boundaries. There must also be a recognized authority and obligation to formally establish security controls over the nongovernmental entities. For example, it is acceptable for a state to leverage an out-of-state private contractor for record archiving and destruction, since access to CHRI by private contractors is authorized pursuant to Title 28, CFR, Section 906, and jurisdictional authority for controls such as audits would be formally established through implementation of the *Security and Management Control Outsourcing Standard for Non-Channelers*.

Public Access

CHRI must not be disseminated to the general public. This includes maintaining CHRI in formats that are accessible by the public or within records that are subject to release through public record requests. However, CHRI may be disclosed as part of the adjudication process during a hearing that is open to the public if the agency demonstrates: 1) the hearing is based on a formally established requirement; 2) the applicant is aware prior to the hearing that CHRI may be disclosed; 3) the applicant is not prohibited from being present at the hearing; and 4) CHRI is not disclosed during the hearing if the applicant withdraws from the application process. For example, a board or commission may be authorized to access CHRI, and as part of regularly scheduled meetings, applicant appeals are discussed as standard agenda items. Even when the specific conditions are met to allow disclosure during a public hearing, the most preferable method for introducing CHRI is to enter into a closed session which limits participation by the public at large. States and local agencies should be able to reasonably demonstrate how the prerequisite criteria are being met for audit purposes.

Additional Considerations

Although not formal categories of assessment, the following considerations are applied to the assessment of requirements for dissemination of CHRI.

General

States need to maintain visibility on the full spectrum of primary agencies to which they disseminate CHRI, as well as the specific purposes/authorities for which those primary agencies receive CHRI. This is especially significant given the requirements for states to execute agency user agreements and establish formal noncriminal justice audit programs in accordance with the *CJIS Security Policy*.

Dissemination of CHRI is broader in concept than the simple act of physically or electronically sending CHRI to a recipient. The concept of dissemination also applies to making CHRI available to recipients through physical or electronic access. The overarching requirements associated with dissemination of CHRI apply regardless of whether CHRI is "pushed" to recipients or "pulled" by recipients since the end result is the same.

Notifications

The definition of CHRI includes information that confirms the existence or nonexistence of CHRI. This includes applicant status information, which is either directly attributed to or predominately based on a national FBI check, when no authority or inherent need

exists for the release of such information. However, if an inherent need does exist to advise a particular entity not otherwise authorized relevant to the federal statutory authority being leveraged for the national criminal history check, then it is acceptable to notify the entity of the outcome of applicant fitness determinations. Entities to which an applicant is seeking employment or licensing may receive status notifications which indicate the positive or negative outcome of fitness determinations. For example, a private day care center is not an authorized recipient of CHRI received pursuant to Public Law 92-544, but may be eligible to receive a status notification regarding an applicant who is seeking employment at the day care center (this assumes of course the approved state statute covers the employment type). States should be able to demonstrate the inherent need for which a particular entity is designated to receive status notifications. Status notifications must not contain CHRI to include confirming the existence or non-existence of CHRI. Generic “pass/fail” language must be used to the greatest extent possible, with the understanding that a reasonable balance must exist between the need to notify a potential employer and not indirectly confirming the existence or non-existence of CHRI. In addition, notification language should not directly reference that a national FBI check was conducted.

Subject of the Record.

Agencies may disseminate fingerprint-based CHRI obtained for noncriminal justice purposes to the subject of the record. It is important to note that agencies are under no direct obligation to provide CHRI to the subject, and dissemination of CHRI by local agencies to the subject may be limited at the state’s discretion. As a best business practice, agencies that disseminate CHRI to the subject of the record should verify the subject’s identity prior to dissemination and document each occurrence. Also, in order to limit potential risks associated with a subject’s subsequent use of a criminal history record, agencies may wish to consider marking the record in some manner to distinguish it as not an original copy.

CHRI may not be disseminated to spouses or other household or family members, even at the subject’s request. Further, CHRI may not be disseminated to other parties such as potential employers on behalf of the subject. However, although the preference is to disseminate directly to the subject of the record, a subject may request that their record be accessed by an attorney acting on the subject’s behalf. This scenario could potentially be encountered when an applicant challenges the outcome of an agency’s fitness determination as part of a formal appeal process.

Residual Access

Other authorized entities also include agencies which require residual access based on oversight authority and responsibility, such as the review of case files by an inspector general’s office or regulatory auditors from outside the receiving organization. Such access should be limited to only the minimum level necessary to accomplish oversight responsibilities, and controls should be established to reasonably prevent unauthorized disclosure of CHRI.

In limited circumstances, government agencies may also be related for the purpose of simply serving as a pass-through for fingerprints and receipt of CHRI. This typically occurs in situations when a criminal justice agency, such as a police department,

performs this specific function on behalf of an authorized recipient. The premise is that “access” to CHRI (view or make use of) is limited to such an extent to essentially consider it negligible for the purposes of formally categorizing it as access.

Purpose for Disclosure of CHRI

The Privacy Act of 1974 requires that the FBI’s CJIS Division keep an accurate accounting of the purpose of each disclosure of a criminal history record and the recipient of that record. (Title 5, U.S.C., Section 552a (c)(1)(A); *III/NFF Operational and Technical Manual*, Chapter 3, Section 2.1)

The NIS audit assesses three categories of requirements for the purpose for disclosure of CHRI: (1) Reason Fingerprinted Field, (2) III Purpose Codes, and (3) Reason for Request.

Reason Fingerprinted Field

All fingerprint-based applicant submissions must include in the reason fingerprinted field an accurate representation of the purpose and/or authority for which the CHRI is to be used.

III Purpose Codes

All name-based III inquiry and record request messages must include the correct purpose code for which the CHRI is to be used.

Reason for Request

All users are required to provide the reason for all name-based and fingerprint-based III transactions upon request by CJIS systems managers, administrators, and representatives. While the purpose code and reason fingerprinted field provide some lead information, they only provide a minimal audit trail. Requiring the specific reason for all III inquiries assists the FBI in ensuring III transactions are conducted for authorized purposes and purpose codes and RFPs are being correctly used. There is also an obligation to ensure requests for CHRI are being conducted for only authorized purposes prior to the submission of the request to the FBI. Submitting entities (e.g., state repositories) are ultimately responsible for ensuring these requirements are met throughout their applicable jurisdictions and should develop the policies, procedures, training, and controls necessary to ensure compliance. While submitting entities should be in a position to indirectly provide or otherwise facilitate providing specific reasons for requests for CHRI during FBI audits, typically local agencies and/or organizational subcomponents that receive and directly use CHRI to adjudicate applications are in the best position to provide specific validating information regarding individual applicants.

Agency identifiers for receipt of CHRI

The inability of an agency to provide a specific reason may be the indirect result of other compliance issues. If an agency receives CHRI for an individual that it has no knowledge of, then there may actually be a dissemination issue. For example, if a state uses a livescan vendor who makes an inaccurate selection of an agency’s Originating Agency Identifier (ORI) or other similar identifier, then the state may send the results to the wrong agency. Unlike the agency that is legitimately waiting for the CHRI, the receiving agency has no knowledge of the applicant and is not able to provide a reason for the submission when asked to do so. As a best business practice, when an agency receives CHRI on an individual that is unknown to the agency, it should inform the state

repository. This practice allows the state repository the opportunity to find out what went wrong with the submission and to ensure that the correct agency is not waiting any longer than necessary for the results of the submission. Submitting entities should also establish effective policies, procedures, and other controls necessary to minimize the risk of inaccuracies with fingerprint submissions that result in the wrong agency receiving CHRI.

Independent application, fingerprinting, and adjudication processes

In a traditional process model, a single agency might be responsible for receiving an individual's application, fingerprinting the applicant, and adjudicating the results of the background check. However, variations on this model have been implemented by agencies, whereby processes associated with receiving an application, obtaining fingerprints, and adjudicating results are independent or "split" from one another and/or performed by a separate entity. These variations may result in applicants being fingerprinted prior to submitting an application. The receipt of fingerprints prior to the application may cause an agency's inability to reasonably assure that the CHRI was for a legitimate purposes and/or the agency may have no knowledge of the applicant. Separate application, fingerprinting, and adjudication processes do not necessarily cause a compliance issue, but oversight agencies must provide sufficient management control to ensure agencies within their jurisdictions that implement such processes have adequate visibility and controls in place to reasonably reduce the risk of unauthorized requests for CHRI and to be able to provide a specific reason for the CHRI request.

Documentation of reason for request

Although agencies must be able to provide CJIS Systems managers, administrators, and representatives some level of specificity about the requests for CHRI in order for them to be "known," there is no direct requirement for an agency to maintain "case files" or other documents in order to support requests for CHRI. In order to meet the requirements for providing a specific reason for requests for CHRI, agencies must have a reasonable level of knowledge of the subject and the specific reason for requesting CHRI for that subject and be able to provide sufficient supporting information, regardless of format. While this is typically accomplished by providing a copy of an application corresponding to a request for CHRI, there are other means by which agencies are able to meet this requirement. A few examples of items that may be used to provide supporting information include: information contained in a personnel database or other information system; copies of online registrations; e-mails showing the purpose or the applicant's position; and supporting statements from applicable officials.

Applicant Notification and Record Challenge

Authorized governmental and nongovernmental agencies/officials that conduct a national fingerprint-based criminal history record check on an applicant for a noncriminal justice purpose (such as employment or a license, immigration or naturalization matter, security clearance, or adoption) are obligated to ensure the applicant is provided certain notice and other information and that the results of the check are handled in a manner that protects the applicant's privacy. Primary references for these requirements include:

-
-
- Title 5, U.S.C., Section 552a (e)(3)
 - Title 28, CFR, Section 50.12
 - Compact Council's Noncriminal Justice Online Policy Resources

The NIS audit assesses three categories of requirements for applicant notification and record challenge: (1) Privacy Act Statement, (2) Opportunity to Complete or Challenge a Record, and (3) Procedures for Obtaining a Record Change.

Privacy Act Statement

Officials must ensure that an applicant receives an adequate Privacy Act statement, when the applicant submits his/her fingerprints and associated personal information. The Privacy Act requires that agencies requesting personally identifiable information provide a Privacy Act statement, which advises individuals of: the authority that permits the solicitation of information; whether the disclosure is mandatory or voluntary; the purpose for which the information will be used; the routine uses which may be made of the information; and the effects of not providing the information. The purpose of this section of the Privacy Act is to facilitate informed consent. An individual should be given enough details about an agency's collection of information to make an informed decision whether to provide the information. The Privacy Act statement can be provided on the FBI Applicant Card (FD-258), another paper form, or electronically, and for efficiency, may be provided in conjunction with the notices required under Title 28, CFR, Section 50.12. It should be noted that providing an adequate Privacy Act statement meets the requirement under Title 28, CFR, Section 50.12 for providing written notification to individuals fingerprinted that the fingerprints will be used to check the criminal history records of the FBI.

The current Privacy Act statement published by the FBI includes the following language:

- **Authority:** The FBI's acquisition, preservation, and exchange of fingerprints and associated information is generally authorized under Title 28, U.S.C., Section 534. Depending on the nature of your application, supplemental authorities include Federal statutes, State statutes pursuant to Public Law 92-544, Presidential Executive Orders, and federal regulations. Providing your fingerprints and associated information is voluntary; however, failure to do so may affect completion or approval of your application.
- **Principal Purpose:** Certain determinations, such as employment, licensing, and security clearances, may be predicated on fingerprint-based background checks. Your fingerprints and associated information/biometrics may be provided to the employing, investigating, or otherwise responsible agency, and/or the FBI for the purpose of comparing your fingerprints to other fingerprints in the FBI's NGI system or its successor systems (including civil, criminal, and latent fingerprint repositories) or other available records of the employing, investigating, or otherwise responsible agency. The FBI may retain your fingerprints and associated information/biometrics in NGI after the completion of this application and, while retained, your fingerprints may continue to be compared against other fingerprints submitted to or retained by NGI.
- **Routine Uses:** During the processing of this application and for as long thereafter as your fingerprints and associated information/biometrics are retained in NGI, your information may be disclosed pursuant to your consent, and may be disclosed without your consent as

permitted by the Privacy Act of 1974 and all applicable Routine Uses as may be published at any time in the Federal Register, including the Routine Uses for the NGI system and the FBI's Blanket Routine Uses. Routine uses include, but are not limited to, disclosures to: employing, governmental or authorized non-governmental agencies responsible for employment, contracting, licensing, security clearances, and other suitability determinations; local, state, tribal, or federal law enforcement agencies; criminal justice agencies; and agencies responsible for national security or public safety.

Opportunity to Complete or Challenge a Record

Officials using the FBI criminal history record (if one exists) to make a determination of the applicant's suitability for the employment, license, or other benefit must provide the applicant the opportunity to complete or challenge the accuracy of the information in the record. Officials should not deny the employment, license, or other benefit based on information in the criminal history record until the applicant has been afforded a reasonable time to correct or complete the record or has declined to do so.

Procedures for Obtaining a Record Change

Officials must advise the applicant that procedures for obtaining a change, correction, or update to an FBI criminal history record are set forth at Title 28, CFR, Section 16.34.

Additional Considerations

Although not formal categories of assessment, the following considerations are applied to the assessment of requirements for applicant notification and record challenge.

The FBI has no objection to officials providing a copy of the applicant's FBI criminal history record to the applicant for review and possible challenge when the record was obtained based on positive fingerprint identification. If agency policy permits, this courtesy will save the applicant the time and additional FBI fee to obtain his/her record directly from the FBI by following the procedures found at Title 28, CFR, Sections 16.30 through 16.34. It will also allow the officials to make a more timely determination of the applicant's suitability.

Each agency should establish and document the process/procedures it utilizes for how/when it gives the applicant notice, what constitutes "a reasonable time" for the applicant to correct or complete the record, and any applicant appeal process that is afforded the applicant. Such documentation will assist State and/or FBI auditors during periodic compliance reviews on use of criminal history records for noncriminal justice purposes.

Noncriminal Justice Agency Audits

Each CJIS Systems Agency, in coordination with the State Identification Bureau, shall establish a process to periodically audit all noncriminal justice agencies, with access to Criminal Justice Information, in order to ensure compliance with applicable statutes, regulations and policies. (*CJIS Security Policy, Section 5.11.2*)

User Fee

Agencies must ensure fingerprint-based requests for CHRI are properly submitted in order to ensure the appropriate application of user fees. Pursuant to Public Law 101-515, the FBI may establish and collect fees to process fingerprint identification records and name checks for noncriminal justice, non-law enforcement employment and licensing purposes.

The NIS audit assesses two categories of requirements for user fee: (1) Criminal Justice and (2) Volunteer.

Criminal Justice (No-fee)

Processing of fingerprint submissions for screening criminal justice agency employees or applicants for employment (sworn and non-sworn) are at no cost inasmuch as criminal justice employment is considered an administration of criminal justice function.

(Title 28, CFR, Section 20.33 (a)(1))

In addition, processing of fingerprint submissions for screening those under contract with criminal justice agencies are at no cost under the following circumstances:

- The contractor is providing services for the administration of criminal justice.
- The contractor is performing services unrelated to the administration of criminal justice, but has unsupervised access to the facility (criminal justice agency site security).

However, fingerprint submissions for screening employees of contractors to whom the entire administration of criminal justice functions have been outsourced, such as private prisons and emergency dispatch centers, are subject to the user fee.

(*Criminal Justice Contract Employee Fingerprint Submission Summary Sheet*, September 2, 2003 and *CJIS Information Letter 07-1*, January 8, 2007)

It should be noted that the definition of “administration of criminal justice” appearing at Title 28, CFR, Section 20.3 (b) includes “Detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders.” However, it is recognized that there are other services which must be performed in support of these nine identified functions and hence, would also be considered an administration of criminal justice function. For example, personnel who transport, feed, provide medical (including psychiatric) care, teach and otherwise engage in the rehabilitative process also perform an administration of criminal justice function, although their functions are only implicitly contained within the regulatory definition.

Volunteer (Reduced-fee)

In the case of a background check conducted with fingerprints on a person who volunteers with a qualified entity, the fees collected by the FBI may not exceed eighteen dollars, or the actual cost, whichever is less. The Type of Search Requested field for applicable fingerprint submission transaction types must be set to a value of “V” to ensure proper processing.

(Title 34, U.S.C., Section 40102 (e); *Electronic Biometric Transmission Specification*, version 10.0.9, Appendix C, page C-40)

Abbreviation or Acronym	Term
Adam Walsh Act	Adam Walsh Child Protection and Safety Act
CFR	Code of Federal Regulations
CHRI	Criminal History Record Information
CJIS	Criminal Justice Information Services
Compact	National Crime Prevention and Privacy Compact
Serve America Act	Edward M. Kennedy Serve America Act
FBI	Federal Bureau of Investigation
III	Interstate Identification Index
NCPA/VCA	National Child Protection Act/Volunteers for Children Act
NFF	National Fingerprint File
NGI	Next Generation Identification
NIS	National Identity Services
ORI	Originating Agency Identifier
U.S.C.	United States Code
VECHS	Volunteer and Employee Criminal History System
WAN	Wide Area Network



Criminal Justice Information Services (CJIS) Security Policy

Version 5.9
06/01/2020

CJISD-ITS-DOC-08140-5.9



Prepared by:
CJIS Information Security Officer

Approved by:
CJIS Advisory Policy Board

EXECUTIVE SUMMARY

Law enforcement needs timely and secure access to services that provide data wherever and whenever for stopping and reducing crime. In response to these needs, the Advisory Policy Board (APB) recommended to the Federal Bureau of Investigation (FBI) that the Criminal Justice Information Services (CJIS) Division authorize the expansion of the existing security management structure in 1998. Administered through a shared management philosophy, the CJIS Security Policy contains information security requirements, guidelines, and agreements reflecting the will of law enforcement and criminal justice agencies for protecting the sources, transmission, storage, and generation of Criminal Justice Information (CJI). The Federal Information Security Management Act of 2002 provides further legal basis for the APB approved management, operational, and technical security requirements mandated to protect CJI and by extension the hardware, software and infrastructure required to enable the services provided by the criminal justice community.

The essential premise of the CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information.

The CJIS Security Policy integrates presidential directives, federal laws, FBI directives and the criminal justice community's APB decisions along with nationally recognized guidance from the National Institute of Standards and Technology. The Policy is presented at both strategic and tactical levels and is periodically updated to reflect the security requirements of evolving business models. The Policy features modular sections enabling more frequent updates to address emerging threats and new security measures. The provided security criteria assists agencies with designing and implementing systems to meet a uniform level of risk and security protection while enabling agencies the latitude to institute more stringent security requirements and controls based on their business model and local needs.

The CJIS Security Policy strengthens the partnership between the FBI and CJIS Systems Agencies (CSA), including, in those states with separate authorities, the State Identification Bureaus (SIB). Further, as use of criminal history record information for noncriminal justice purposes continues to expand, the CJIS Security Policy becomes increasingly important in guiding the National Crime Prevention and Privacy Compact Council and State Compact Officers in the secure exchange of criminal justice records.

The Policy describes the vision and captures the security concepts that set the policies, protections, roles, and responsibilities with minimal impact from changes in technology. The Policy empowers CSAs with the insight and ability to tune their security programs according to their risks, needs, budgets, and resource constraints while remaining compliant with the baseline level of security set forth in this Policy. The CJIS Security Policy provides a secure framework of laws, standards, and elements of published and vetted policies for accomplishing the mission across the broad spectrum of the criminal justice and noncriminal justice communities.

CHANGE MANAGEMENT

Revision	Change Description	Created/Changed by	Date	Approved By
5	Policy Rewrite	Security Policy Working Group	2/9/2011	See Signature Page
5.1	Incorporate Calendar Year 2011 APB approved changes and administrative changes	CJIS ISO Program Office	7/13/2012	APB & Compact Council
5.2	Incorporate Calendar Year 2012 APB approved changes and administrative changes	CJIS ISO Program Office	8/9/2013	APB & Compact Council
5.3	Incorporate Calendar Year 2013 APB approved changes and administrative changes	CJIS ISO Program Office	8/4/2014	APB & Compact Council
5.4	Incorporate Calendar Year 2014 APB approved changes and administrative changes	CJIS ISO Program Office	10/6/2015	APB & Compact Council
5.5	Incorporate Calendar Year 2015 APB approved changes and administrative changes	CJIS ISO Program Office	6/1/2016	APB & Compact Council
5.6	Incorporate Calendar Year 2016 APB approved changes and administrative changes	CJIS ISO Program Office	6/5/2017	APB & Compact Council
5.7	Incorporate Calendar Year 2017 APB approved changes and administrative changes	CJIS ISO Program Office	08/16/2018	APB & Compact Council
5.8	Incorporate Calendar Year 2018 APB approved changes and administrative changes	CJIS ISO Program Office	06/01/2019	APB & Compact Council
5.9	Incorporate Calendar Year 2019 APB approved changes and administrative changes	CJIS ISO Program Office	06/01/2020	APB & Compact Council

SUMMARY OF CHANGES

Version 5.9

APB Approved Changes

1. **Section 5.13.2 Mobile Device Management (MDM):** add clarifying language, Fall 2019, APB#18, SA#3, Mobile Device Management (MDM) Requirements in the *CJIS Security Policy*.
2. **Appendix H, Security Addendum:** add example of contract addendum, Fall 2019, APB#18, SA#7, Audit of Vendor Contracts with Authorized Criminal Justice Agencies (CJAs).
3. **NOTE:** There were no Spring 2019 APB actions.

Administrative Changes¹

1. **Section 5.6.2.2.2 Advanced Authentication Decision Tree:** updated the tree description to account for direct and indirect access to CJI.
2. **Figures 9 and 10:** updated both figures to account for direct and indirect access to CJI.

KEY TO APB APPROVED CHANGES (e.g. “Fall 2013, APB#11, SA#6, add language, Future CSP for Mobile Devices”):

Fall 2013 – Advisory Policy Board cycle and year

APB# – Advisory Policy Board Topic number

SA# – Security and Access Subcommittee Topic number

Summary of change

Topic title

¹ Administrative changes are vetted through the Security and Access Subcommittee and not the entire APB process.

TABLE OF CONTENTS

Executive Summary	i
Change Management	ii
Summary of Changes	iii
Table of Contents	iv
List of Figures	ix
1 Introduction	1
1.1 Purpose	1
1.2 Scope	1
1.3 Relationship to Local Security Policy and Other Policies	1
1.4 Terminology Used in This Document	2
1.5 Distribution of the CJIS Security Policy	2
2 CJIS Security Policy Approach	3
2.1 CJIS Security Policy Vision Statement	3
2.2 Architecture Independent	3
2.3 Risk Versus Realism	3
3 Roles and Responsibilities	4
3.1 Shared Management Philosophy	4
3.2 Roles and Responsibilities for Agencies and Parties	4
3.2.1 CJIS Systems Agencies (CSA)	5
3.2.2 CJIS Systems Officer (CSO)	5
3.2.3 Terminal Agency Coordinator (TAC)	6
3.2.4 Criminal Justice Agency (CJA)	6
3.2.5 Noncriminal Justice Agency (NCJA)	6
3.2.6 Contracting Government Agency (CGA)	7
3.2.7 Agency Coordinator (AC)	7
3.2.8 CJIS Systems Agency Information Security Officer (CSA ISO)	7
3.2.9 Local Agency Security Officer (LASO)	8
3.2.10 FBI CJIS Division Information Security Officer (FBI CJIS ISO)	8
3.2.11 Repository Manager	9
3.2.12 Compact Officer	9
4 Criminal Justice Information and Personally Identifiable Information	10
4.1 Criminal Justice Information (CJI)	10
4.1.1 Criminal History Record Information (CHRI)	10
4.2 Access, Use and Dissemination of Criminal History Record Information (CHRI), NCIC Restricted Files Information, and NCIC Non-Restricted Files Information	11
4.2.1 Proper Access, Use, and Dissemination of CHRI	11
4.2.2 Proper Access, Use, and Dissemination of NCIC Restricted Files Information	11
4.2.3 Proper Access, Use, and Dissemination of NCIC Non-Restricted Files Information	11
4.2.3.1 For Official Purposes	11
4.2.3.2 For Other Authorized Purposes	12
4.2.3.3 CSO Authority in Other Circumstances	12
4.2.4 Storage	12
4.2.5 Justification and Penalties	12

4.2.5.1	Justification	12
4.2.5.2	Penalties	12
4.3	Personally Identifiable Information (PII).....	12
5	Policy and Implementation	14
5.1	Policy Area 1: Information Exchange Agreements	15
5.1.1	Information Exchange	15
5.1.1.1	Information Handling.....	15
5.1.1.2	State and Federal Agency User Agreements	15
5.1.1.3	Criminal Justice Agency User Agreements	16
5.1.1.4	Interagency and Management Control Agreements	16
5.1.1.5	Private Contractor User Agreements and CJIS Security Addendum.....	16
5.1.1.6	Agency User Agreements	17
5.1.1.7	Outsourcing Standards for Channelers	17
5.1.1.8	Outsourcing Standards for Non-Channelers	18
5.1.2	Monitoring, Review, and Delivery of Services	18
5.1.2.1	Managing Changes to Service Providers	18
5.1.3	Secondary Dissemination.....	18
5.1.4	Secondary Dissemination of Non-CHRI CJI	18
5.2	Policy Area 2: Security Awareness Training.....	20
5.2.1	Basic Security Awareness Training	20
5.2.1.1	Level One Security Awareness Training	20
5.2.1.2	Level Two Security Awareness Training	20
5.2.1.3	Level Three Security Awareness Training	21
5.2.1.4	Level Four Security Awareness Training	21
5.2.2	LASO Training.....	22
5.2.3	Security Training Records.....	22
5.3	Policy Area 3: Incident Response	24
5.3.1	Reporting Security Events.....	24
5.3.1.1	Reporting Structure and Responsibilities.....	24
5.3.1.1.1	FBI CJIS Division Responsibilities	24
5.3.1.1.2	CSA ISO Responsibilities.....	24
5.3.2	Management of Security Incidents.....	25
5.3.2.1	Incident Handling.....	25
5.3.2.2	Collection of Evidence.....	25
5.3.3	Incident Response Training.....	25
5.3.4	Incident Monitoring.....	25
5.4	Policy Area 4: Auditing and Accountability.....	27
5.4.1	Auditable Events and Content (Information Systems).....	27
5.4.1.1	Events.....	27
5.4.1.1.1	Content.....	28
5.4.2	Response to Audit Processing Failures	28
5.4.3	Audit Monitoring, Analysis, and Reporting.....	28
5.4.4	Time Stamps.....	28
5.4.5	Protection of Audit Information	28
5.4.6	Audit Record Retention.....	28
5.4.7	Logging NCIC and III Transactions.....	29

5.5	Policy Area 5: Access Control.....	30
5.5.1	Account Management	30
5.5.2	Access Enforcement.....	30
5.5.2.1	Least Privilege	31
5.5.2.2	System Access Control	31
5.5.2.3	Access Control Criteria.....	31
5.5.2.4	Access Control Mechanisms.....	31
5.5.3	Unsuccessful Login Attempts	32
5.5.4	System Use Notification.....	32
5.5.5	Session Lock	32
5.5.6	Remote Access	33
5.5.6.1	Personally Owned Information Systems.....	33
5.5.6.2	Publicly Accessible Computers	33
5.6	Policy Area 6: Identification and Authentication	35
5.6.1	Identification Policy and Procedures.....	35
5.6.1.1	Use of Originating Agency Identifiers in Transactions and Information Exchanges	35
5.6.2	Authentication Policy and Procedures	35
5.6.2.1	Standard Authenticators.....	36
5.6.2.1.1	Password	36
5.6.2.1.2	Personal Identification Number (PIN)	38
5.6.2.1.3	One-time Passwords (OTP)	38
5.6.2.2	Advanced Authentication.....	38
5.6.2.2.1	Advanced Authentication Policy and Rationale	39
5.6.2.2.2	Advanced Authentication Decision Tree	39
5.6.3	Identifier and Authenticator Management	41
5.6.3.1	Identifier Management.....	41
5.6.3.2	Authenticator Management.....	42
5.6.4	Assertions	42
5.7	Policy Area 7: Configuration Management	48
5.7.1	Access Restrictions for Changes	48
5.7.1.1	Least Functionality.....	48
5.7.1.2	Network Diagram.....	48
5.7.2	Security of Configuration Documentation	48
5.8	Policy Area 8: Media Protection.....	49
5.8.1	Media Storage and Access	49
5.8.2	Media Transport	49
5.8.2.1	Digital Media during Transport	49
5.8.2.2	Physical Media in Transit	49
5.8.3	Digital Media Sanitization and Disposal.....	49
5.8.4	Disposal of Physical Media.....	49
5.9	Policy Area 9: Physical Protection	51
5.9.1	Physically Secure Location	51
5.9.1.1	Security Perimeter.....	51
5.9.1.2	Physical Access Authorizations	51
5.9.1.3	Physical Access Control	51

5.9.1.4	Access Control for Transmission Medium	51
5.9.1.5	Access Control for Display Medium	51
5.9.1.6	Monitoring Physical Access	52
5.9.1.7	Visitor Control	52
5.9.1.8	Delivery and Removal	52
5.9.2	Controlled Area	52
5.10	Policy Area 10: System and Communications Protection and Information Integrity	53
5.10.1	Information Flow Enforcement	53
5.10.1.1	Boundary Protection	53
5.10.1.2	Encryption.....	54
5.10.1.2.1	Encryption for CJI in Transit	54
5.10.1.2.2	Encryption for CJI at Rest.....	55
5.10.1.2.3	Public Key Infrastructure (PKI) Technology.....	55
5.10.1.3	Intrusion Detection Tools and Techniques	55
5.10.1.4	Voice over Internet Protocol.....	56
5.10.1.5	Cloud Computing.....	56
5.10.2	Facsimile Transmission of CJI.....	57
5.10.3	Partitioning and Virtualization	57
5.10.3.1	Partitioning.....	57
5.10.3.2	Virtualization	58
5.10.4	System and Information Integrity Policy and Procedures.....	58
5.10.4.1	Patch Management.....	58
5.10.4.2	Malicious Code Protection.....	59
5.10.4.3	Spam and Spyware Protection	59
5.10.4.4	Security Alerts and Advisories	59
5.10.4.5	Information Input Restrictions.....	60
5.11	Policy Area 11: Formal Audits	61
5.11.1	Audits by the FBI CJIS Division.....	61
5.11.1.1	Triennial Compliance Audits by the FBI CJIS Division	61
5.11.1.2	Triennial Security Audits by the FBI CJIS Division	61
5.11.2	Audits by the CSA.....	61
5.11.3	Special Security Inquiries and Audits	62
5.11.4	Compliance Subcommittees	62
5.12	Policy Area 12: Personnel Security	63
5.12.1	Personnel Screening Requirements for Individuals Requiring Unescorted Access to Unencrypted CJI	63
5.12.2	Personnel Termination	64
5.12.3	Personnel Transfer.....	64
5.12.4	Personnel Sanctions.....	64
5.13	Policy Area 13: Mobile Devices	66
5.13.1	Wireless Communications Technologies	66
5.13.1.1	802.11 Wireless Protocols	66
5.13.1.2	Cellular Devices.....	67
5.13.1.2.1	Cellular Service Abroad.....	68
5.13.1.2.2	Voice Transmissions Over Cellular Devices	68
5.13.1.3	Bluetooth.....	68

5.13.1.4 Mobile Hotspots.....	68
5.13.2 Mobile Device Management (MDM)	69
5.13.3 Wireless Device Risk Mitigations	69
5.13.4 System Integrity	70
5.13.4.1 Patching/Updates	70
5.13.4.2 Malicious Code Protection.....	70
5.13.4.3 Personal Firewall	70
5.13.5 Incident Response	71
5.13.6 Access Control	71
5.13.7 Identification and Authentication.....	71
5.13.7.1 Local Device Authentication	71
5.13.7.2 Advanced Authentication.....	72
5.13.7.2.1 Compensating Controls.....	72
5.13.7.3 Device Certificates.....	72
Appendices.....	A-1
Appendix A Terms and Definitions	A-1
Appendix B Acronyms.....	B-1
Appendix C Network Topology Diagrams	C-1
Appendix D Sample Information Exchange Agreements.....	D-1
D.1 CJIS User Agreement	D-1
D.2 Management Control Agreement.....	D-9
D.3 Noncriminal Justice Agency Agreement & Memorandum of Understanding.....	D-10
D.4 Interagency Connection Agreement	D-16
Appendix E Security Forums and Organizational Entities.....	E-1
Appendix F Sample Forms.....	F-1
F.1 Security Incident Response Form	F-2
Appendix G Best practices.....	G-1
G.1 Virtualization	G-1
G.2 Voice over Internet Protocol.....	G-4
G.3 Cloud Computing.....	G-15
G.4 Mobile Appendix	G-32
G.5 Administrator Accounts for Least Privilege and Separation of Duties.....	G-53
G.6 Encryption.....	G-66
G.7 Incident Response	G-76
G.8 Secure Coding.....	G-89
Appendix H Security Addendum	H-1
Appendix I References.....	I-1
Appendix J Noncriminal Justice Agency Supplemental Guidance	J-1
Appendix K Criminal Justice Agency Supplemental Guidance	K-1

LIST OF FIGURES

Figure 1 – Overview Diagram of Strategic Functions and Policy Components.....	4
Figure 2 – Dissemination of restricted and non-restricted NCIC data.....	13
Figure 3 – Information Exchange Agreements Implemented by a Local Police Department	19
Figure 4 – Security Awareness Training Use Cases.....	22
Figure 5 – Incident Response Process Initiated by an Incident in a Local Police Department	26
Figure 6 – Local Police Department's Use of Audit Logs	29
Figure 7 – A Local Police Department's Access Controls	34
Figure 8 – Advanced Authentication Use Cases.....	42
Figure 9 – Authentication Decision for Known Location	46
Figure 10 – Authentication Decision for Unknown Location	47
Figure 11 – A Local Police Department's Configuration Management Controls	48
Figure 12 – A Local Police Department's Media Management Policies.....	50
Figure 13 – A Local Police Department's Physical Protection Measures.....	52
Figure 14 – System and Communications Protection and Information Integrity Use Cases.....	60
Figure 15 – The Audit of a Local Police Department.....	62
Figure 16 – A Local Police Department's Personnel Security Controls	64

1 INTRODUCTION

This section details the purpose of this document, its scope, relationship to other information security policies, and its distribution constraints.

1.1 Purpose

The CJIS Security Policy provides Criminal Justice Agencies (CJA) and Noncriminal Justice Agencies (NCJA) with a minimum set of security requirements for access to Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division systems and information and to protect and safeguard Criminal Justice Information (CJI). This minimum standard of security requirements ensures continuity of information protection. The essential premise of the CJIS Security Policy is to provide the appropriate controls to protect CJI, from creation through dissemination; whether at rest or in transit.

The CJIS Security Policy integrates presidential directives, federal laws, FBI directives, the criminal justice community's Advisory Policy Board (APB) decisions along with nationally recognized guidance from the National Institute of Standards and Technology (NIST) and the National Crime Prevention and Privacy Compact Council (Compact Council).

1.2 Scope

At the consent of the advisory process, and taking into consideration federal law and state statutes, the CJIS Security Policy applies to all entities with access to, or who operate in support of, FBI CJIS Division's services and information. The CJIS Security Policy provides minimum security requirements associated with the creation, viewing, modification, transmission, dissemination, storage, or destruction of CJI.

Entities engaged in the interstate exchange of CJI data for noncriminal justice purposes are also governed by the standards and rules promulgated by the Compact Council.

1.3 Relationship to Local Security Policy and Other Policies

The CJIS Security Policy may be used as the sole security policy for the agency. The local agency may complement the CJIS Security Policy with a local policy, or the agency may develop their own stand-alone security policy; however, the CJIS Security Policy shall always be the minimum standard and local policy may augment, or increase the standards, but shall not detract from the CJIS Security Policy standards.

The agency shall develop, disseminate, and maintain formal, documented procedures to facilitate the implementation of the CJIS Security Policy and, where applicable, the local security policy. The policies and procedures shall be consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidance. Procedures developed for CJIS Security Policy areas can be developed for the security program in general, and for a particular information system, when required.

This document is a compendium of applicable policies in providing guidance on the minimum security controls and requirements needed to access FBI CJIS information and services. These policies include presidential directives, federal laws, FBI directives and the criminal justice community's APB decisions. State, local, and Tribal CJA may implement more stringent policies

and requirements. Appendix I contains the references while Appendix E lists the security forums and organizational entities referenced in this document.

1.4 Terminology Used in This Document

The following terms are used interchangeably throughout this document:

- **Agency and Organization:** The two terms in this document refer to any entity that submits or receives information, by any means, to/from FBI CJIS systems or services.
- **Information and Data:** Both terms refer to CJI.
- **System, Information System, Service, or named applications like NCIC:** all refer to connections to the FBI's criminal justice information repositories and the equipment used to establish said connections.
- **References/Citations/Directives:** Appendix I contains all of the references used in this Policy and may contain additional sources that could apply to any section.

Appendix A and B provide an extensive list of the terms and acronyms.

1.5 Distribution of the CJIS Security Policy

The CJIS Security Policy, version 5.0 and later, is a publically available document and may be posted and shared without restrictions.

2 CJIS SECURITY POLICY APPROACH

The CJIS Security Policy represents the shared responsibility between FBI CJIS, CJIS Systems Agency (CSA), and the State Identification Bureaus (SIB) of the lawful use and appropriate protection of CJI. The Policy provides a baseline of security requirements for current and planned services and sets a minimum standard for new initiatives.

2.1 CJIS Security Policy Vision Statement

The executive summary of this document describes the vision in terms of business needs for confidentiality, integrity, and availability of information. The APB collaborates with the FBI CJIS Division to ensure that the Policy remains updated to meet evolving business, technology and security needs.

2.2 Architecture Independent

Due to advancing technology and evolving business models, the FBI CJIS Division is transitioning from legacy stovepipe systems and moving toward a flexible services approach. Systems such as National Crime Information Center (NCIC), National Instant Criminal Background Check System (NICS), and Next Generation Identification (NGI) will continue to evolve and may no longer retain their current system platforms, hardware, or program name. However, the data and services provided by these systems will remain stable.

The CJIS Security Policy looks at the data (information), services, and protection controls that apply regardless of the implementation architecture. Architectural independence is not intended to lessen the importance of systems, but provide for the replacement of one technology with another while ensuring the controls required to protect the information remain constant. This objective and conceptual focus on security policy areas provide the guidance and standards while avoiding the impact of the constantly changing landscape of technical innovations. The architectural independence of the Policy provides agencies with the flexibility for tuning their information security infrastructure and policies to reflect their own environments.

2.3 Risk Versus Realism

Every “shall” statement contained within the CJIS Security Policy has been scrutinized for risk versus the reality of resource constraints and real-world application. The purpose of the CJIS Security Policy is to establish the minimum security requirements; therefore, individual agencies are encouraged to implement additional controls to address agency specific risks. Each agency faces risk unique to that agency. It is quite possible that several agencies could encounter the same type of risk however depending on resources would mitigate that risk differently. In that light, a risk-based approach can be used when implementing requirements.

3 ROLES AND RESPONSIBILITIES

3.1 Shared Management Philosophy

In the scope of information security, the FBI CJIS Division employs a shared management philosophy with federal, state, local, and tribal law enforcement agencies. Although an advisory policy board for the NCIC has existed since 1969, the Director of the FBI established the CJIS APB in March 1994 to enable appropriate input and recommend policy with respect to CJIS services. Through the APB and its Subcommittees and Working Groups, consideration is given to the needs of the criminal justice and law enforcement community regarding public policy, statutory and privacy aspects, as well as national security relative to CJIS systems and information. The APB represents federal, state, local, and tribal law enforcement and criminal justice agencies throughout the United States, its territories, and Canada.

The FBI has a similar relationship with the Compact Council, which governs the interstate exchange of criminal history records for noncriminal justice purposes. The Compact Council is mandated by federal law to promulgate rules and procedures for the use of the Interstate Identification Index (III) for noncriminal justice purposes. To meet that responsibility, the Compact Council depends on the CJIS Security Policy as the definitive source for standards defining the security and privacy of records exchanged with noncriminal justice practitioners.

3.2 Roles and Responsibilities for Agencies and Parties

It is the responsibility of all agencies covered under this Policy to ensure the protection of CJI between the FBI CJIS Division and its user community. The following figure provides an abstract representation of the strategic functions and roles such as governance and operations.

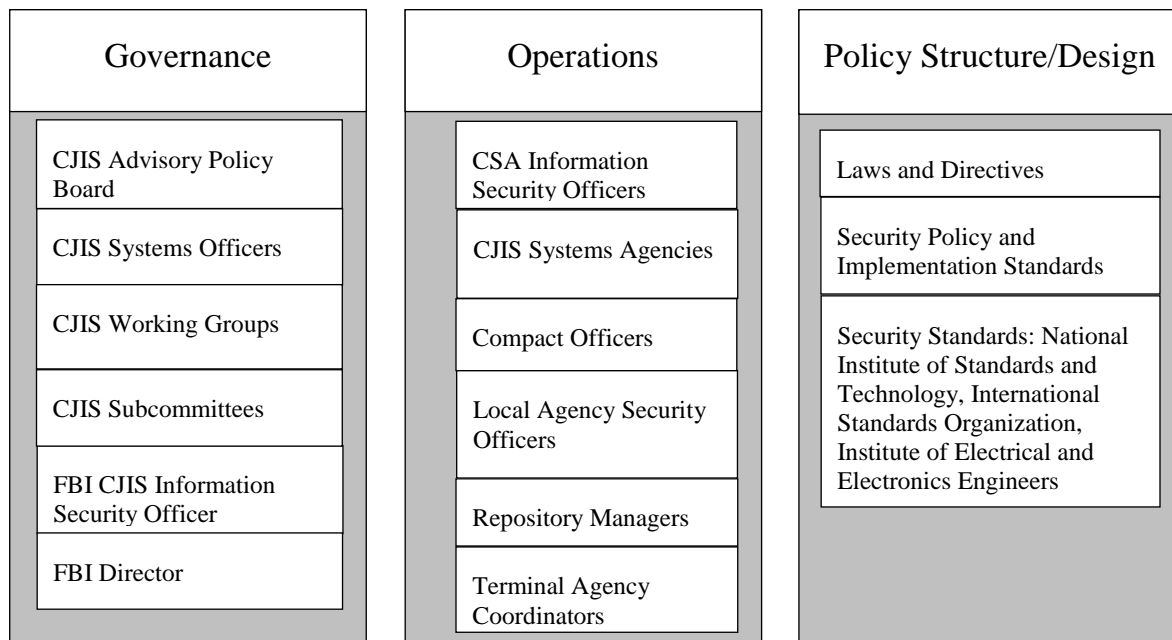


Figure 1 – Overview Diagram of Strategic Functions and Policy Components

This section provides a description of the following entities and roles:

1. CJIS Systems Agency.
2. CJIS Systems Officer.
3. Terminal Agency Coordinator.
4. Criminal Justice Agency.
5. Noncriminal Justice Agency.
6. Contracting Government Agency.
7. Agency Coordinator.
8. CJIS Systems Agency Information Security Officer.
9. Local Agency Security Officer.
10. FBI CJIS Division Information Security Officer.
11. Repository Manager.
12. Compact Officer.

3.2.1 CJIS Systems Agencies (CSA)

The CSA is responsible for establishing and administering an information technology security program throughout the CSA's user community, to include the local levels. The head of each CSA shall appoint a CJIS Systems Officer (CSO). The CSA may impose more stringent protection measures than outlined in this document. Such decisions shall be documented and kept current.

3.2.2 CJIS Systems Officer (CSO)

The CSO is an individual located within the CSA responsible for the administration of the CJIS network for the CSA. Pursuant to the Bylaws for the CJIS Advisory Policy Board and Working Groups, the role of CSO shall not be outsourced. The CSO may delegate responsibilities to subordinate agencies. The CSO shall set, maintain, and enforce the following:

1. Standards for the selection, supervision, and separation of personnel who have access to CJIS.
2. Policy governing the operation of computers, access devices, circuits, hubs, routers, firewalls, and other components that comprise and support a telecommunications network and related CJIS systems used to process, store, or transmit CJIS, guaranteeing the priority, confidentiality, integrity, and availability of service needed by the criminal justice community.
 - a. Ensure appropriate use, enforce system discipline, and ensure CJIS Division operating procedures are followed by all users of the respective services and information.
 - b. Ensure state/federal agency compliance with policies approved by the APB and adopted by the FBI.

- c. Ensure the appointment of the CSA ISO and determine the extent of authority to the CSA ISO.
 - d. Ensure the designation of a Terminal Agency Coordinator (TAC) within each agency with devices accessing CJIS systems.
 - e. Ensure each agency having access to CJI has someone designated as the Local Agency Security Officer (LASO).
 - f. Ensure each LASO receives enhanced security awareness training (ref. Section 5.2).
 - g. Approve access to FBI CJIS systems.
 - h. Assume ultimate responsibility for managing the security of CJIS systems within their state and/or agency.
 - i. Perform other related duties outlined by the user agreements with the FBI CJIS Division.
3. Outsourcing of Criminal Justice Functions
- a. Responsibility for the management of the approved security requirements shall remain with the CJA. Security control includes the authority to enforce the standards for the selection, supervision, and separation of personnel who have access to CJI; set and enforce policy governing the operation of computers, circuits, and telecommunications terminals used to process, store, or transmit CJI; and to guarantee the priority service needed by the criminal justice community.
 - b. Responsibility for the management control of network security shall remain with the CJA. Management control of network security includes the authority to enforce the standards for the selection, supervision, and separation of personnel who have access to CJI; set and enforce policy governing the operation of circuits and network equipment used to transmit CJI; and to guarantee the priority service as determined by the criminal justice community.

3.2.3 Terminal Agency Coordinator (TAC)

The TAC serves as the point-of-contact at the local agency for matters relating to CJIS information access. The TAC administers CJIS systems programs within the local agency and oversees the agency's compliance with CJIS systems policies.

3.2.4 Criminal Justice Agency (CJA)

A CJA is defined as a court, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspectors General Offices are included.

3.2.5 Noncriminal Justice Agency (NCJA)

A NCJA is defined (for the purposes of access to CJI) as an entity or any subunit thereof that provides services primarily for purposes other than the administration of criminal justice.

3.2.6 Contracting Government Agency (CGA)

A CGA is a government agency, whether a CJA or a NCJA, that enters into an agreement with a private contractor subject to the CJIS Security Addendum. The CGA entering into an agreement with a contractor shall appoint an agency coordinator.

3.2.7 Agency Coordinator (AC)

An AC is a staff member of the CGA who manages the agreement between the Contractor and agency. The AC shall be responsible for the supervision and integrity of the system, training and continuing education of employees and operators, scheduling of initial training and testing, and certification testing and all required reports by NCIC. The AC shall:

1. Understand the communications, records capabilities, and needs of the Contractor which is accessing federal and state records through or because of its relationship with the CGA.
2. Participate in related meetings and provide input and comments for system improvement.
3. Receive information from the CGA (e.g., system updates) and disseminate it to appropriate Contractor employees.
4. Maintain and update manuals applicable to the effectuation of the agreement, and provide them to the Contractor.
5. Maintain up-to-date records of Contractor's employees who access the system, including name, date of birth, social security number, date fingerprint card(s) submitted, date security clearance issued, and date initially trained, tested, certified or recertified (if applicable).
6. Train or ensure the training of Contractor personnel. If Contractor personnel access NCIC, schedule the operators for testing or a certification exam with the CSA staff, or AC staff with permission from the CSA staff. Schedule new operators for the certification exam within six (6) months of assignment. Schedule certified operators for biennial re-certification testing within thirty (30) days prior to the expiration of certification. Schedule operators for other mandated class.
7. The AC will not permit an untrained/untested or non-certified Contractor employee to access CJI or systems supporting CJI where access to CJI can be gained.
8. Where appropriate, ensure compliance by the Contractor with NCIC validation requirements.
9. Provide completed applicant fingerprint cards on each Contractor employee who accesses the system to the CGA (or, where appropriate, CSA) for criminal background investigation prior to such employee accessing the system.
10. Any other responsibility for the AC promulgated by the FBI.

3.2.8 CJIS Systems Agency Information Security Officer (CSA ISO)

The CSA ISO shall:

1. Serve as the security point of contact (POC) to the FBI CJIS Division ISO.

2. Document technical compliance with the CJIS Security Policy with the goal to assure the confidentiality, integrity, and availability of criminal justice information to the user community throughout the CSA's user community, to include the local level.
3. Document and provide assistance for implementing the security-related controls for the Interface Agency and its users.
4. Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CSA, the affected criminal justice agency, and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI.

3.2.9 Local Agency Security Officer (LASO)

Each LASO shall:

1. Identify who is using the CSA approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
2. Identify and document how the equipment is connected to the state system.
3. Ensure that personnel security screening procedures are being followed as stated in this Policy.
4. Ensure the approved and appropriate security measures are in place and working as expected.
5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

3.2.10 FBI CJIS Division Information Security Officer (FBI CJIS ISO)

The FBI CJIS ISO shall:

1. Maintain the CJIS Security Policy.
2. Disseminate the FBI Director approved CJIS Security Policy.
3. Serve as a liaison with the CSA's ISO and with other personnel across the CJIS community and in this regard provide technical guidance as to the intent and implementation of operational and technical policy issues.
4. Serve as a point-of-contact (POC) for computer incident notification and distribution of security alerts to the CSOs and ISOs.
5. Assist with developing audit compliance guidelines as well as identifying and reconciling security-related issues.
6. Develop and participate in information security training programs for the CSOs and ISOs, and provide a means by which to acquire feedback to measure the effectiveness and success of such training.
7. Maintain a security policy resource center (SPRC) on FBI.gov and keep the CSOs and ISOs updated on pertinent information.

3.2.11 Repository Manager

The State Identification Bureau (SIB) Chief, i.e. Repository Manager or Chief Administrator, is the designated manager of the agency having oversight responsibility for a state's fingerprint identification services. If both state fingerprint identification services and CJIS systems control are managed within the same state agency, the SIB Chief and CSO may be the same person.

3.2.12 Compact Officer

Pursuant to the National Crime Prevention and Privacy Compact, each party state shall appoint a Compact Officer who shall ensure that Compact provisions and rules, procedures, and standards established by the Compact Council are complied with in their respective state.

4 CRIMINAL JUSTICE INFORMATION AND PERSONALLY IDENTIFIABLE INFORMATION

4.1 Criminal Justice Information (CJI)

Criminal Justice Information is the term used to refer to all of the FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data. The following categories of CJI describe the various data sets housed by the FBI CJIS architecture:

1. Biometric Data—data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. Used to identify individuals, to include: fingerprints, palm prints, iris scans, and facial recognition data.
2. Identity History Data—textual data that corresponds with an individual’s biometric data, providing a history of criminal and/or civil events for the identified individual.
3. Biographic Data—information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.
4. Property Data—information about vehicles and property associated with crime when accompanied by any personally identifiable information (PII).
5. Case/Incident History—information about the history of criminal incidents.

The following type of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g., ORI, NIC, UCN, etc.) when not accompanied by information that reveals CJI or PII.

The intent of the CJIS Security Policy is to ensure the protection of the aforementioned CJI until the information is: released to the public via authorized dissemination (e.g. within a court system; presented in crime reports data; released in the interest of public safety); purged or destroyed in accordance with applicable record retention rules. CJI introduced into the court system pursuant to a judicial proceeding that can be released to the public via a public records request is not subject to the CJIS Security Policy.

4.1.1 Criminal History Record Information (CHRI)

Criminal History Record Information (CHRI), sometimes informally referred to as “restricted data”, is a subset of CJI. Due to its comparatively sensitive nature, additional controls are required for the access, use and dissemination of CHRI. In addition to the dissemination restrictions outlined below, Title 28, Part 20, Code of Federal Regulations (CFR), defines CHRI and provides the regulatory guidance for dissemination of CHRI. While the CJIS Security Policy attempts to be architecturally independent, the III and the NCIC are specifically identified in Title 28, Part 20, CFR, and the NCIC Operating Manual, as associated with CHRI.

4.2 Access, Use and Dissemination of Criminal History Record Information (CHRI), NCIC Restricted Files Information, and NCIC Non-Restricted Files Information

This section describes the requirements for the access, use and dissemination of CHRI, NCIC restricted files information, and NCIC non-restricted files information.

4.2.1 Proper Access, Use, and Dissemination of CHRI

Information obtained from the III is considered CHRI. Rules governing the access, use, and dissemination of CHRI are found in Title 28, Part 20, CFR. The III shall be accessed only for an authorized purpose. Further, CHRI shall only be used for an authorized purpose consistent with the purpose for which III was accessed. Dissemination to another agency is authorized if (a) the other agency is an Authorized Recipient of such information and is being serviced by the accessing agency, or (b) the other agency is performing personnel and appointment functions for criminal justice employment applicants.

4.2.2 Proper Access, Use, and Dissemination of NCIC Restricted Files Information

The NCIC hosts restricted files and non-restricted files. NCIC restricted files are distinguished from NCIC non-restricted files by the policies governing their access and use. Proper access to, use, and dissemination of data from restricted files shall be consistent with the access, use, and dissemination policies concerning the III described in Title 28, Part 20, CFR, and the NCIC Operating Manual. The restricted files, which shall be protected as CHRI, are as follows:

1. Gang Files
2. Known or Appropriately Suspected Terrorist Files
3. Supervised Release Files
4. National Sex Offender Registry Files
5. Historical Protection Order Files of the NCIC
6. Identity Theft Files
7. Protective Interest Files
8. Person With Information (PWI) data in the Missing Person Files
9. Violent Person File
10. NICS Denied Transactions File

The remaining NCIC files are considered non-restricted files.

4.2.3 Proper Access, Use, and Dissemination of NCIC Non-Restricted Files Information

4.2.3.1 For Official Purposes

NCIC non-restricted files are those not listed as restricted files in Section 4.2.2. NCIC non-restricted files information may be accessed and used for any authorized purpose consistent with

the inquiring agency's responsibility. Information obtained may be disseminated to (a) other government agencies or (b) private entities authorized by law to receive such information for any purpose consistent with their responsibilities.

4.2.3.2 For Other Authorized Purposes

NCIC non-restricted files may be accessed for other purposes consistent with the resources of the inquiring agency; however, requests for bulk data are discouraged. Information derived from NCIC non-restricted files for other than law enforcement purposes can be used by authorized criminal justice personnel only to confirm the status of a person or property (i.e., wanted or stolen). An inquiring agency is authorized to charge a nominal administrative fee for such service. Non-restricted files information shall not be disseminated commercially.

A response to a NCIC person inquiry may include NCIC restricted files information as well as NCIC non-restricted files information. Agencies shall not disseminate restricted files information for purposes other than law enforcement.

4.2.3.3 CSO Authority in Other Circumstances

If no federal, state or local law or policy prohibition exists, the CSO may exercise discretion to approve or deny dissemination of NCIC non-restricted file information.

4.2.4 Storage

When CHRI is stored, agencies shall establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of the information. These records shall be stored for extended periods only when they are key elements for the integrity and/or utility of case files and/or criminal record files. See Section 5.9 for physical security controls.

4.2.5 Justification and Penalties

4.2.5.1 Justification

In addition to the use of purpose codes and logging information, all users shall provide a reason for all III inquiries whenever requested by NCIC System Managers, CSAs, local agency administrators, or their representatives.

4.2.5.2 Penalties

Improper access, use or dissemination of CHRI and NCIC Non-Restricted Files information is serious and may result in administrative sanctions including, but not limited to, termination of services and state and federal criminal penalties.

4.3 Personally Identifiable Information (PII)

For the purposes of this document, PII is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. Any FBI CJIS provided data maintained by an agency, including but not limited to, education, financial transactions, medical history, and criminal or employment history may include PII. A criminal history record for

example inherently contains PII as would a Law Enforcement National Data Exchange (N-DEx) case file.

PII shall be extracted from CJI for the purpose of official business only. Agencies shall develop policies, based on state and local privacy rules, to ensure appropriate controls are applied when handling PII extracted from CJI. Due to the expansive nature of PII, this Policy does not specify auditing, logging, or personnel security requirements associated with the life cycle of PII.

Figure 2 – Dissemination of restricted and non-restricted NCIC data

A citizen of Springfield went to the Springfield Police Department to request whether his new neighbor, who had been acting suspiciously, had an outstanding warrant. The Springfield Police Department ran an NCIC persons inquiry, which produced a response that included a Wanted Person File (non-restricted file) record and a Known or Appropriately Suspected Terrorist File (restricted file) record. The Springfield Police Department advised the citizen of the outstanding warrant, but did not disclose any information concerning the subject being a known or appropriately suspected terrorist.

5 POLICY AND IMPLEMENTATION

The policy areas focus upon the data and services that the FBI CJIS Division exchanges and provides to the criminal justice community and its partners. Each policy area provides both strategic reasoning and tactical implementation requirements and standards.

While the major theme of the policy areas is concerned with electronic exchange directly with the FBI, it is understood that further dissemination of CJI to Authorized Recipients by various means (hard copy, e-mail, web posting, etc.) constitutes a significant portion of CJI exchanges. Regardless of its form, use, or method of dissemination, CJI requires protection throughout its life.

Not every consumer of FBI CJIS services will encounter all of the policy areas therefore the circumstances of applicability are based on individual agency/entity configurations and usage. Use cases within each of the policy areas will help users relate the Policy to their own agency circumstances. The policy areas are:

- Policy Area 1—Information Exchange Agreements
- Policy Area 2—Security Awareness Training
- Policy Area 3—Incident Response
- Policy Area 4—Auditing and Accountability
- Policy Area 5—Access Control
- Policy Area 6—Identification and Authentication
- Policy Area 7—Configuration Management
- Policy Area 8—Media Protection
- Policy Area 9—Physical Protection
- Policy Area 10—Systems and Communications Protection and Information Integrity
- Policy Area 11—Formal Audits
- Policy Area 12—Personnel Security
- Policy Area 13—Mobile Devices

5.1 Policy Area 1: Information Exchange Agreements

The information shared through communication mediums shall be protected with appropriate security safeguards. The agreements established by entities sharing information across systems and communications mediums are vital to ensuring all parties fully understand and agree to a set of security standards.

5.1.1 Information Exchange

Before exchanging CJI, agencies shall put formal agreements in place that specify security controls. The exchange of information may take several forms including electronic mail, instant messages, web services, facsimile, hard copy, and information systems sending, receiving and storing CJI.

Information exchange agreements outline the roles, responsibilities, and data ownership between agencies and any external parties. Information exchange agreements for agencies sharing CJI data that is sent to and/or received from the FBI CJIS shall specify the security controls and conditions described in this document.

Information exchange agreements shall be supported by documentation committing both parties to the terms of information exchange. As described in subsequent sections, different agreements and policies apply, depending on whether the parties involved are CJAs or NCJAs. See Appendix D for examples of Information Exchange Agreements.

There may be instances, on an ad-hoc basis, where CJI is authorized for further dissemination to Authorized Recipients not covered by an information exchange agreement with the releasing agency. In these instances the dissemination of CJI is considered to be secondary dissemination. Law Enforcement and civil agencies shall have a local policy to validate a requestor of CJI as an authorized recipient before disseminating CJI. See Section 5.1.3 for secondary dissemination guidance.

5.1.1.1 Information Handling

Procedures for handling and storage of information shall be established to protect that information from unauthorized disclosure, alteration or misuse. Using the requirements in this Policy as a starting point, the procedures shall apply to the handling, processing, storing, and communication of CJI. These procedures apply to the exchange of CJI no matter the form of exchange.

The policies for information handling and protection also apply to using CJI shared with or received from FBI CJIS for noncriminal justice purposes. In general, a noncriminal justice purpose includes the use of criminal history records for purposes authorized by federal or state law other than purposes relating to the administration of criminal justice, including – but not limited to - employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

5.1.1.2 State and Federal Agency User Agreements

Each CSA head or SIB Chief shall execute a signed written user agreement with the FBI CJIS Division stating their willingness to demonstrate conformity with this Policy before accessing and participating in CJIS records information programs. This agreement shall include the standards and sanctions governing utilization of CJIS systems. As coordinated through the particular CSA

or SIB Chief, each Interface Agency shall also allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system. All user agreements with the FBI CJIS Division shall be coordinated with the CSA head.

5.1.1.3 Criminal Justice Agency User Agreements

Any CJA receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA providing the access. The written agreement shall specify the FBI CJIS systems and services to which the agency will have access, and the FBI CJIS Division policies to which the agency must adhere. These agreements shall include:

1. Audit.
2. Dissemination.
3. Hit confirmation.
4. Logging.
5. Quality Assurance (QA).
6. Screening (Pre-Employment).
7. Security.
8. Timeliness.
9. Training.
10. Use of the system.
11. Validation.

5.1.1.4 Interagency and Management Control Agreements

A NCJA (government) designated to perform criminal justice functions for a CJA shall be eligible for access to the CJI. Access shall be permitted when such designation is authorized pursuant to executive order, statute, regulation, or interagency agreement. The NCJA shall sign and execute a management control agreement (MCA) with the CJA, which stipulates management control of the criminal justice function remains solely with the CJA. The MCA may be a separate document or included with the language of an interagency agreement. An example of an NCJA (government) is a city information technology (IT) department.

5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum

The CJIS Security Addendum is a uniform addendum to an agreement between the government agency and a private contractor, approved by the Attorney General of the United States, which specifically authorizes access to CHRI, limits the use of the information to the purposes for which it is provided, ensures the security and confidentiality of the information is consistent with existing regulations and the CJIS Security Policy, provides for sanctions, and contains such other provisions as the Attorney General may require.

Private contractors who perform criminal justice functions shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies. All private contractors who perform criminal justice functions shall acknowledge, via signing of the CJIS Security

Addendum Certification page, and abide by all aspects of the CJIS Security Addendum. The CJIS Security Addendum is presented in Appendix H. Modifications to the CJIS Security Addendum shall be enacted only by the FBI.

1. Private contractors designated to perform criminal justice functions for a CJA shall be eligible for access to CJI. Access shall be permitted pursuant to an agreement which specifically identifies the agency's purpose and scope of providing services for the administration of criminal justice. The agreement between the CJA and the private contractor shall incorporate the CJIS Security Addendum approved by the Director of the FBI, acting for the U.S. Attorney General, as referenced in Title 28 CFR 20.33 (a)(7).
2. Private contractors designated to perform criminal justice functions on behalf of a NCJA (government) shall be eligible for access to CJI. Access shall be permitted pursuant to an agreement which specifically identifies the agency's purpose and scope of providing services for the administration of criminal justice. The agreement between the NCJA and the private contractor shall incorporate the CJIS Security Addendum approved by the Director of the FBI, acting for the U.S. Attorney General, as referenced in Title 28 CFR 20.33 (a)(7).

5.1.1.6 Agency User Agreements

A NCJA (public) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions, shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. A NCJA (public) receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA/SIB providing the access. An example of a NCJA (public) is a county school board.

A NCJA (private) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions, shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. A NCJA (private) receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA, SIB, or authorized agency providing the access. An example of a NCJA (private) is a local bank.

All NCJAs accessing CJI shall be subject to all pertinent areas of the CJIS Security Policy (see Appendix J for supplemental guidance). Each NCJA that directly accesses FBI CJI shall also allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system.

5.1.1.7 Outsourcing Standards for Channelers

Channelers designated to request civil fingerprint-based background checks or noncriminal justice ancillary functions on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. All Channelers accessing CJI shall be subject to the terms and conditions described in the Compact

Council Security and Management Control Outsourcing Standard. Each Channeler that directly accesses CJI shall also allow the FBI to conduct periodic penetration testing.

Channelers leveraging CJI to perform civil functions on behalf of an Authorized Recipient shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies.

5.1.1.8 Outsourcing Standards for Non-Channelers

Contractors designated to perform noncriminal justice ancillary functions on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. All contractors accessing CJI shall be subject to the terms and conditions described in the Compact Council Outsourcing Standard for Non-Channelers. Contractors leveraging CJI to perform civil functions on behalf of an Authorized Recipient shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies.

5.1.2 Monitoring, Review, and Delivery of Services

As specified in the interagency agreements, MCAs, and contractual agreements with private contractors, the services, reports and records provided by the service provider shall be regularly monitored and reviewed. The CJA, authorized agency, or FBI shall maintain sufficient overall control and visibility into all security aspects to include, but not limited to, identification of vulnerabilities and information security incident reporting/response. The incident reporting/response process used by the service provider shall conform to the incident reporting/response specifications provided in this Policy.

5.1.2.1 Managing Changes to Service Providers

Any changes to services provided by a service provider shall be managed by the CJA, authorized agency, or FBI. This includes provision of services, changes to existing services, and new services. Evaluation of the risks to the agency shall be undertaken based on the criticality of the data, system, and the impact of the change.

5.1.3 Secondary Dissemination

If CHRI is released to another authorized agency, and that agency was not part of the releasing agency's primary information exchange agreement(s), the releasing agency shall log such dissemination.

5.1.4 Secondary Dissemination of Non-CHRI CJI

If CJI does not contain CHRI and is not part of an information exchange agreement then it does not need to be logged. Dissemination shall conform to the local policy validating the requestor of the CJI as an employee and/or contractor of a law enforcement agency or civil agency requiring the CJI to perform their mission or a member of the public receiving CJI via authorized dissemination.

Figure 3 – Information Exchange Agreements Implemented by a Local Police Department

A local police department executed a Memorandum of Understanding (MOU) for the interface with their state CSA. The local police department also executed an MOU (which included an MCA) with the county information technology (IT) department for the day-to-day operations of their criminal-justice infrastructure. The county IT department, in turn, outsourced operations to a local vendor who signed the CJIS Security Addendum.

5.2 Policy Area 2: Security Awareness Training

Security training is key to the human element of information security. All users with authorized access to CJI should be made aware of their individual responsibilities and expected behavior when accessing CJI and the systems which process CJI. LASOs require enhanced training on the specific duties and responsibilities of those positions and the impact those positions have on the overall security of information systems.

5.2.1 Basic Security Awareness Training

Basic security awareness training shall be required within six months of initial assignment, and biennially thereafter, for all personnel who have access to CJI to include all personnel who have unescorted access to a physically secure location. The CSO/SIB Chief may accept the documentation of the completion of security awareness training from another agency. Accepting such documentation from another agency means that the accepting agency assumes the risk that the training may not meet a particular requirement or process required by federal, state, or local laws.

A significant number of topics can be mentioned and briefly discussed in any awareness session or campaign. To help further the development and implementation of individual agency security awareness training programs the following baseline guidance is provided.

5.2.1.1 Level One Security Awareness Training

At a minimum, the following topics shall be addressed as baseline security awareness training for all personnel who have unescorted access to a physically secure location:

1. Individual responsibilities and expected behavior with regard to being in the vicinity of CJI usage and/or terminals.
2. Implications of noncompliance.
3. Incident response (Identify points of contact and individual actions).
4. Visitor control and physical access to spaces—discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity, etc.

5.2.1.2 Level Two Security Awareness Training

In addition to 5.2.1.1 above, the following topics, at a minimum, shall be addressed as baseline security awareness training for all authorized personnel with access to CJI:

1. Media protection.
2. Protect information subject to confidentiality concerns — hardcopy through destruction.
3. Proper handling and marking of CJI.
4. Threats, vulnerabilities, and risks associated with handling of CJI.
5. Social engineering.
6. Dissemination and destruction.

5.2.1.3 Level Three Security Awareness Training

In addition to 5.2.1.1 and 5.2.1.2 above, the following topics, at a minimum, shall be addressed as baseline security awareness training for all authorized personnel with both physical and logical access to CJIS:

1. Rules that describe responsibilities and expected behavior with regard to information system usage.
2. Password usage and management—including creation, frequency of changes, and protection.
3. Protection from viruses, worms, Trojan horses, and other malicious code.
4. Unknown e-mail/attachments.
5. Web usage—allowed versus prohibited; monitoring of user activity.
6. Spam.
7. Physical Security—increases in risks to systems and data.
8. Handheld device security issues—address both physical and wireless security issues.
9. Use of encryption and the transmission of sensitive/confidential information over the Internet—address agency policy, procedures, and technical contact for assistance.
10. Laptop security—address both physical and information security issues.
11. Personally owned equipment and software—state whether allowed or not (e.g., copyrights).
12. Access control issues—address least privilege and separation of duties.
13. Individual accountability—explain what this means in the agency.
14. Use of acknowledgement statements—passwords, access to systems and data, personal use and gain.
15. Desktop security—discuss use of screensavers, restricting visitors' view of information on screen (mitigating “shoulder surfing”), battery backup devices, allowed access to systems.
16. Protect information subject to confidentiality concerns—in systems, archived, on backup media, and until destroyed.
17. Threats, vulnerabilities, and risks associated with accessing CJIS Service systems and services.

5.2.1.4 Level Four Security Awareness Training

In addition to 5.2.1.1, 5.2.1.2, and 5.1.2.3 above, the following topics at a minimum shall be addressed as baseline security awareness training for all Information Technology personnel (system administrators, security administrators, network administrators, etc.):

1. Protection from viruses, worms, Trojan horses, and other malicious code—scanning, updating definitions.
2. Data backup and storage—centralized or decentralized approach.

3. Timely application of system patches—part of configuration management.
4. Access control measures.
5. Network infrastructure protection measures.

5.2.2 LASO Training

LASO training shall be required prior to assuming duties but no later than six months after initial assignment, and annually thereafter.

At a minimum, the following topics shall be addressed as enhanced security awareness training for a LASO:

1. The roles and responsibilities listed in CJIS Security Policy Section 3.2.9.
2. Additional state/local/tribal/federal agency LASO roles and responsibilities.
3. Summary of audit findings from previous state audits of local agencies.
4. Findings from the last FBI CJIS Division audit of the CSA.
5. Most recent changes to the CJIS Security Policy.

5.2.3 Security Training Records

Records of individual basic security awareness training and specific information system security training shall be documented, kept current, and maintained by the CSO/SIB Chief/Compact Officer. Maintenance of training records can be delegated to the local level.

Figure 4 – Security Awareness Training Use Cases

Use Case 1 - Security Awareness Training Program Implementation by a Local Police Department

A local police department with a staff of 20 sworn criminal justice professionals and 15 support personnel worked with a vendor to develop role-specific security-awareness training, and required all staff to complete this training upon assignment and every two years thereafter. The local police department scheduled the sworn law-enforcement training to coincide with their NCIC certification training. The vendor maintained the training records for the police department’s entire staff, and provided reporting to the department to help it ensure compliance with the CJIS Security Policy.

Use Case 2 - Level One Security Awareness Training

A local police department hires custodial staff that will have physical access throughout the PD (a physically secure location) after normal business hours to clean the facility. These personnel have unescorted access to a physically secure location and therefore must be given the baseline security awareness training on all the topics identified in CSP Section 5.2.1.1 Level One Security Awareness Training.

Use Case 3 – Level Two Security Awareness Training

A school district maintains a locked file cabinet with hard copies of background check results of all teachers and employees which may include CJI (CHRI). Only authorized personnel who have the

ability to open the cabinet are required to be given the baseline security awareness training on all the topics identified in CSP Sections 5.2.1.1 and 5.2.1.2.

Use Case 4 – Level Three Security Awareness Training

A County Sheriff's Office has employed a number of dispatchers. Part of the function of these dispatchers is to run CJI queries at the request of the Sheriff and deputies. As part of their daily duties, the dispatchers have access to CJI both logically (running queries) and physically (printed copies of reports containing CJI). These dispatchers are entrusted with direct access to CJI and are therefore required to be given the baseline security awareness training on all the topics identified in CSP Sections 5.2.1.1, 5.2.1.2, and 5.2.1.3.

Use Case 5 – Level Four Security Awareness Training

The State Police has hired a number of system and network administrator personnel to help bolster security of the state network. Part of their daily duties may include creating accounts for new personnel, implementing security patches for existing systems, creating backups of existing systems, and implementing access controls throughout the network. These administrators have privileged access to CJI and CJI-processing systems, and are therefore required to be given the baseline security awareness training on all the topics identified in CSP Sections 5.2.1.1, 5.2.1.2, 5.2.1.3, and 5.2.1.4.

5.3 Policy Area 3: Incident Response

The security risk of both accidental and malicious attacks against government and private agencies, remains persistent in both physical and logical environments. To ensure protection of CJI, agencies shall: (i) establish operational incident handling procedures that include adequate preparation, detection, analysis, containment, recovery, and user response activities; (ii) track, document, and report incidents to appropriate agency officials and/or authorities.

ISOs have been identified as the POC on security-related issues for their respective agencies and shall ensure LASOs institute the CSA incident response reporting procedures at the local level. Appendix F contains a sample incident notification letter for use when communicating the details of a CJI-related incident to the FBI CJIS ISO.

Refer to Section 5.13.5 for additional incident response requirements related to mobile devices used to access CJI.

5.3.1 Reporting Security Events

The agency shall promptly report incident information to appropriate authorities. Security events, including identified weaknesses associated with the event, shall be communicated in a manner allowing timely corrective action to be taken. Formal event reporting and escalation procedures shall be in place. Wherever feasible, the agency shall employ automated mechanisms to assist in the reporting of security incidents. All employees, contractors and third party users shall be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of agency assets and are required to report any security events and weaknesses as quickly as possible to the designated point of contact.

5.3.1.1 Reporting Structure and Responsibilities

5.3.1.1.1 FBI CJIS Division Responsibilities

The FBI CJIS Division shall:

1. Manage and maintain the CJIS Division's Computer Security Incident Response Capability (CSIRC).
2. Serve as a central clearinghouse for all reported intrusion incidents, security alerts, bulletins, and other security-related material.
3. Ensure additional resources for all incidents affecting FBI CJIS Division controlled systems as needed.
4. Disseminate prompt advisories of system threats and operating system vulnerabilities via the security policy resource center on FBI.gov, to include but not limited to: Product Security Bulletins, Virus Bulletins, and Security Clips.
5. Track all reported incidents and/or trends.
6. Monitor the resolution of all incidents.

5.3.1.1.2 CSA ISO Responsibilities

The CSA ISO shall:

1. Assign individuals in each state, federal, and international law enforcement organization to be the primary point of contact for interfacing with the FBI CJIS Division concerning incident handling and response.
2. Identify individuals who are responsible for reporting incidents within their area of responsibility.
3. Collect incident information from those individuals for coordination and sharing among other organizations that may or may not be affected by the incident.
4. Develop, implement, and maintain internal incident response procedures and coordinate those procedures with other organizations that may or may not be affected.
5. Collect and disseminate all incident-related information received from the Department of Justice (DOJ), FBI CJIS Division, and other entities to the appropriate local law enforcement POCs within their area.
6. Act as a single POC for their jurisdictional area for requesting incident response assistance.

5.3.2 Management of Security Incidents

A consistent and effective approach shall be applied to the management of security incidents. Responsibilities and procedures shall be in place to handle security events and weaknesses effectively once they have been reported.

5.3.2.1 Incident Handling

The agency shall implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. Wherever feasible, the agency shall employ automated mechanisms to support the incident handling process.

Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. The agency should incorporate the lessons learned from ongoing incident handling activities into the incident response procedures and implement the procedures accordingly.

5.3.2.2 Collection of Evidence

Where a follow-up action against a person or agency after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

5.3.3 Incident Response Training

The agency shall ensure general incident response roles responsibilities are included as part of required security awareness training.

5.3.4 Incident Monitoring

The agency shall track and document security incidents on an ongoing basis. The CSA ISO shall maintain completed security incident reporting forms until the subsequent FBI triennial audit or until legal action (if warranted) is complete; whichever time-frame is greater.

Figure 5 – Incident Response Process Initiated by an Incident in a Local Police Department

A state ISO received a notification from a local police department that suspicious network activity from a known botnet was detected on their network. The state ISO began the process of collecting all pertinent information about this incident, e.g. incident date/time, points-of-contact, systems affected, nature of the incident, actions taken, etc. and requested that the local police department confirm that their malware signatures were up to date. The state ISO contacted both the FBI CJIS ISO and state CSO to relay the preliminary details of this incident. The FBI CJIS ISO instructed the involved parties to continue their investigation and to submit an incident response form once all the information had been gathered. The FBI CJIS ISO contacted the lead for the FBI CSIRC to inform them that an incident response form was forthcoming. The state ISO gathered the remainder of the information from the local police department and submitted a completed incident response form to the FBI CJIS ISO who subsequently provided it to the FBI CSIRC. The FBI CSIRC notified the Department of Justice Computer Incident Response Team (DOJCIRT). The state ISO continued to monitor the situation, passing relevant details to the FBI CJIS ISO, ultimately determining that the botnet was eliminated from the local police department's infrastructure. Subsequent investigations determined that the botnet was restricted to the department's administrative infrastructure and thus no CJIS was compromised.

5.4 Policy Area 4: Auditing and Accountability

Agencies shall implement audit and accountability controls to increase the probability of authorized users conforming to a prescribed pattern of behavior. Agencies shall carefully assess the inventory of components that compose their information systems to determine which security controls are applicable to the various components.

Auditing controls are typically applied to the components of an information system that provide auditing capability (servers, etc.) and would not necessarily be applied to every user-level workstation within the agency. As technology advances, more powerful and diverse functionality can be found in such devices as personal digital assistants and cellular telephones, which may require the application of security controls in accordance with an agency assessment of risk.

Refer to Section 5.13.6 for additional audit requirements related to mobile devices used to access CJJ.

5.4.1 Auditable Events and Content (Information Systems)

The agency's information system shall generate audit records for defined events. These defined events include identifying significant events which need to be audited as relevant to the security of the information system. The agency shall specify which information system components carry out auditing activities. Auditing activity can affect information system performance and this issue must be considered as a separate factor during the acquisition of information systems.

The agency's information system shall produce, at the application and/or operating system level, audit records containing sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. The agency shall periodically review and update the list of agency-defined auditable events. In the event an agency does not use an automated system, manual recording of activities shall still take place.

5.4.1.1 Events

The following events shall be logged:

1. Successful and unsuccessful system log-on attempts.
2. Successful and unsuccessful attempts to use:
 - a. access permission on a user account, file, directory or other system resource;
 - b. create permission on a user account, file, directory or other system resource;
 - c. write permission on a user account, file, directory or other system resource;
 - d. delete permission on a user account, file, directory or other system resource;
 - e. change permission on a user account, file, directory or other system resource.
3. Successful and unsuccessful attempts to change account passwords.
4. Successful and unsuccessful actions by privileged accounts (i.e. root, Oracle, DBA, admin, etc.).
5. Successful and unsuccessful attempts for users to:
 - a. access the audit log file;

- b. modify the audit log file;
- c. destroy the audit log file.

5.4.1.1.1 Content

The following content shall be included with every audited event:

1. Date and time of the event.
2. The component of the information system (e.g., software component, hardware component) where the event occurred.
3. Type of event.
4. User/subject identity.
5. Outcome (success or failure) of the event.

5.4.2 Response to Audit Processing Failures

The agency's information system shall provide alerts to appropriate agency officials in the event of an audit processing failure. Audit processing failures include, for example: software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

5.4.3 Audit Monitoring, Analysis, and Reporting

The responsible management official shall designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions. Audit review/analysis shall be conducted at a minimum once a week. The frequency of review/analysis should be increased when the volume of an agency's processing indicates an elevated need for audit review. The agency shall increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to agency operations, agency assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

5.4.4 Time Stamps

The agency's information system shall provide time stamps for use in audit record generation. The time stamps shall include the date and time values generated by the internal system clocks in the audit records. The agency shall synchronize internal information system clocks on an annual basis.

5.4.5 Protection of Audit Information

The agency's information system shall protect audit information and audit tools from modification, deletion and unauthorized access.

5.4.6 Audit Record Retention

The agency shall retain audit records for at least one (1) year. Once the minimum retention time period has passed, the agency shall continue to retain audit records until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for

example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions.

5.4.7 Logging NCIC and III Transactions

A log shall be maintained for a minimum of one (1) year on all NCIC and III transactions. The III portion of the log shall clearly identify both the operator and the authorized receiving agency. III logs shall also clearly identify the requester and the secondary recipient. The identification on the log shall take the form of a unique identifier that shall remain unique to the individual requester and to the secondary recipient throughout the minimum one year retention period.

Figure 6 – Local Police Department's Use of Audit Logs

A state CSO contacted a local police department regarding potentially inappropriate use of CHRI that was retrieved using the local department's ORI. The state CSO requested all relevant information from the police department to reconcile state NCIC and III logs against local police department logs. The police department provided the combination of their CJJ processing application's logs with relevant operating system and network infrastructure logs to help verify the identity of the users conducting these queries. The review of these logs substantiated the CSO's suspicion.

5.5 Policy Area 5: Access Control

Access control provides the planning and implementation of mechanisms to restrict reading, writing, processing and transmission of CJIS information and the modification of information systems, applications, services and communication configurations allowing access to CJIS information.

Refer to Section 5.13.6 for additional access control requirements related to mobile devices used to access CJIS.

5.5.1 Account Management

The agency shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The agency shall validate information system accounts at least annually and shall document the validation process. The validation and documentation of accounts can be delegated to local agencies.

Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The agency shall identify authorized users of the information system and specify access rights/privileges. The agency shall grant access to the information system based on:

1. Valid need-to-know/need-to-share that is determined by assigned official duties.
2. Satisfaction of all personnel security criteria.

The agency responsible for account creation shall be notified when:

1. A user's information system usage or need-to-know or need-to-share changes.
2. A user is terminated or transferred or associated accounts are removed, disabled, or otherwise secured.

5.5.2 Access Enforcement

The information system shall enforce assigned authorizations for controlling access to the system and contained information. The information system controls shall restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.

Explicitly authorized personnel include, for example, security administrators, system and network administrators, and other privileged users with access to system control, monitoring, or administration functions (e.g., system administrators, information system security officers, maintainers, system programmers).

Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) shall be employed by agencies to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system.

5.5.2.1 Least Privilege

The agency shall approve individual access privileges and shall enforce physical and logical access restrictions associated with changes to the information system; and generate, retain, and review records reflecting all such changes. The agency shall enforce the most restrictive set of rights/privileges or access needed by users for the performance of specified tasks. The agency shall implement least privilege based on specific duties, operations, or information systems as necessary to mitigate risk to CJI. This limits access to CJI to only authorized personnel with the need and the right to know.

Logs of access privilege changes shall be maintained for a minimum of one year or at least equal to the agency's record retention policy – whichever is greater.

5.5.2.2 System Access Control

Access control mechanisms to enable access to CJI shall be restricted by object (e.g., data set, volumes, files, records) including the ability to read, write, or delete the objects. Access controls shall be in place and operational for all IT systems to:

1. Prevent multiple concurrent active sessions for one user identification, for those applications accessing CJI, unless the agency grants authority based upon operational business needs. Agencies shall document the parameters of the operational business needs for multiple concurrent active sessions.
2. Ensure that only authorized personnel can add, change, or remove component devices, dial-up connections, and remove or alter programs.

5.5.2.3 Access Control Criteria

Agencies shall control access to CJI based on one or more of the following:

1. Job assignment or function (i.e., the role) of the user seeking access.
2. Physical location.
3. Logical location.
4. Network addresses (e.g., users from sites within a given agency may be permitted greater access than those from outside).
5. Time-of-day and day-of-week/month restrictions.

5.5.2.4 Access Control Mechanisms

When setting up access controls, agencies shall use one or more of the following mechanisms:

1. Access Control Lists (ACLs). ACLs are a register of users (including groups, machines, processes) who have been given permission to use a particular object (system resource) and the types of access they have been permitted.
2. Resource Restrictions. Access to specific functions is restricted by never allowing users to request information, functions, or other resources for which they do not have access. Three major types of resource restrictions are: menus, database views, and network devices.

3. Encryption. Encrypted information can only be decrypted, and therefore read, by those possessing the appropriate cryptographic key. While encryption can provide strong access control, it is accompanied by the need for strong key management. Follow the guidance in Section 5.10.1.2 for encryption requirements if encryption of stored information is employed as an access enforcement mechanism.
4. Application Level. In addition to controlling access at the information system level, access enforcement mechanisms are employed at the application level to provide increased information security for the agency.

5.5.3 Unsuccessful Login Attempts

Where technically feasible, the system shall enforce a limit of no more than 5 consecutive invalid access attempts by a user (attempting to access CJI or systems with access to CJI). The system shall automatically lock the account/node for a 10 minute time period unless released by an administrator.

5.5.4 System Use Notification

The information system shall display an approved system use notification message, before granting access, informing potential users of various usages and monitoring rules. The system use notification message shall, at a minimum, provide the following information:

1. The user is accessing a restricted information system.
2. System usage may be monitored, recorded, and subject to audit.
3. Unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties.
4. Use of the system indicates consent to monitoring and recording.

The system use notification message shall provide appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remain on the screen until the user acknowledges the notification and takes explicit actions to log on to the information system.

Privacy and security policies shall be consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidance. System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. For publicly accessible systems:

1. the system use information is available and when appropriate, is displayed before granting access;
2. any references to monitoring, recording, or auditing are in keeping with privacy accommodations for such systems that generally prohibit those activities; and
3. the notice given to public users of the information system includes a description of the authorized uses of the system.

5.5.5 Session Lock

The information system shall prevent further access to the system by initiating a session lock after a maximum of 30 minutes of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures. Users shall

directly initiate session lock mechanisms to prevent inadvertent viewing when a device is unattended. A session lock is not a substitute for logging out of the information system. In the interest of safety, devices that are: (1) part of a criminal justice conveyance; or (2) used to perform dispatch functions and located within a physically secure location; or (3) terminals designated solely for the purpose of receiving alert notifications (i.e. receive only terminals or ROT) used within physically secure location facilities that remain staffed when in operation, are exempt from this requirement. Note: an example of a session lock is a screen saver with password.

5.5.6 Remote Access

The agency shall authorize, monitor, and control all methods of remote access to the information system. Remote access is any temporary access to an agency's information system by a user (or an information system) communicating temporarily through an external, non-agency-controlled network (e.g., the Internet).

The agency shall employ automated mechanisms to facilitate the monitoring and control of remote access methods. The agency shall control all remote accesses through managed access control points. The agency may permit remote access for privileged functions only for compelling operational needs but shall document the technical and administrative process for enabling remote access for privileged functions in the security plan for the information system.

Virtual escorting of privileged functions is permitted only when all the following conditions are met:

1. The session shall be monitored at all times by an authorized escort
2. The escort shall be familiar with the system/area in which the work is being performed.
3. The escort shall have the ability to end the session at any time.
4. The remote administrative personnel connection shall be via an encrypted (FIPS 140-2 certified) path.
5. The remote administrative personnel shall be identified prior to access and authenticated prior to or during the session. This authentication may be accomplished prior to the session via an Advanced Authentication (AA) solution or during the session via active teleconference with the escort throughout the session.

5.5.6.1 Personally Owned Information Systems

A personally owned information system shall not be authorized to access, process, store or transmit CJI unless the agency has established and documented the specific terms and conditions for personally owned information system usage. When personally owned mobile devices (i.e. bring your own device [BYOD]) are authorized, they shall be controlled in accordance with the requirements in Policy Area 13: Mobile Devices.

This control does not apply to the use of personally owned information systems to access agency's information systems and information that are intended for public access (e.g., an agency's public website that contains purely public information).

5.5.6.2 Publicly Accessible Computers

Publicly accessible computers shall not be used to access, process, store or transmit CJI. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

Figure 7 – A Local Police Department’s Access Controls

A local police department purchased a new computer-assisted dispatch (CAD) system that integrated with their state CSA’s CJI interfaces. In doing so, the police department employed least-privilege practices to ensure that its employees were only given those privileges needed to perform their jobs, and as such, excluding IT administrators, employees had only non-administrative privileges on all equipment they used. The police department also used ACLs in the operating systems to control access to the CAD client’s executables. The CAD system used internal role-based access controls to ensure only those users that needed access to CJI were given it. The police department performed annual audits of user accounts on all systems under their control including remote access mechanisms, operating systems, and the CAD system to ensure all accounts were in valid states. The police department implemented authentication-failure account lockouts, system use notification via login banners, and screen-saver passwords on all equipment that processes CJI.

5.6 Policy Area 6: Identification and Authentication

The agency shall identify information system users and processes acting on behalf of users and authenticate the identities of those users or processes as a prerequisite to allowing access to agency information systems or services.

5.6.1 Identification Policy and Procedures

Each person who is authorized to store, process, and/or transmit CJI shall be uniquely identified. A unique identification shall also be required for all persons who administer and maintain the system(s) that access CJI or networks leveraged for CJI transit. The unique identification can take the form of a full name, badge number, serial number, or other unique alphanumeric identifier. Agencies shall require users to identify themselves uniquely before the user is allowed to perform any actions on the system. Agencies shall ensure that all user IDs belong to currently authorized users. Identification data shall be kept current by adding new users and disabling and/or deleting former users.

5.6.1.1 Use of Originating Agency Identifiers in Transactions and Information Exchanges

An FBI authorized originating agency identifier (ORI) shall be used in each transaction on CJIS systems in order to identify the sending agency and to ensure the proper level of access for each transaction. The original identifier between the requesting agency and the CSA/SIB/Channeler shall be the ORI, and other agency identifiers, such as user identification or personal identifier, an access device mnemonic, or the Internet Protocol (IP) address.

Agencies may act as a servicing agency and perform transactions on behalf of authorized agencies requesting the service. Servicing agencies performing inquiry transactions on behalf of another agency may do so using the requesting agency's ORI. Servicing agencies may also use their own ORI to perform inquiry transactions on behalf of a requesting agency if the means and procedures are in place to provide an audit trail for the current specified retention period. Because the agency performing the transaction may not necessarily be the same as the agency requesting the transaction, the CSA/SIB/Channeler shall ensure that the ORI for each transaction can be traced, via audit trail, to the specific agency which is requesting the transaction.

Audit trails can be used to identify the requesting agency if there is a reason to inquire into the details surrounding why an agency ran an inquiry on a subject. Agencies assigned a P (limited access) ORI shall not use the full access ORI of another agency to conduct an inquiry transaction.

5.6.2 Authentication Policy and Procedures

Authentication refers to mechanisms or processes that verify users are valid once they are uniquely identified. The CSA/SIB may develop an authentication strategy which centralizes oversight but decentralizes the establishment and daily administration of the security measures for access to CJI.

Each individual's identity shall be authenticated at either the local agency, CSA, SIB or Channeler level. The authentication strategy shall be part of the agency's audit for policy compliance. The FBI CJIS Division shall identify and authenticate all individuals who establish direct web-based interactive sessions with FBI CJIS Services. The FBI CJIS Division shall authenticate the ORI of all message-based sessions between the FBI CJIS Division and its customer agencies but will not

further authenticate the user nor capture the unique identifier for the originating operator because this function is performed at the local agency, CSA, SIB or Channeler level.

5.6.2.1 Standard Authenticators

Authenticators are (the something you know, something you are, or something you have) part of the identification and authentication process. Examples of standard authenticators include passwords, hard or soft tokens, biometrics, one-time passwords (OTP) and personal identification numbers (PIN). Users shall not be allowed to use the same password or PIN in the same logon sequence.

5.6.2.1.1 Password

When agencies use a password as an authenticator for an individual's unique ID, they shall use the basic password standards in 5.6.2.1.1.1, OR follow the advanced password standards in 5.6.2.1.1.2.

NOTE: There is no option to combine or select particular options between the two separate lists below.

5.6.2.1.1.1 Basic Password Standards

When agencies elect to follow the basic password standards, passwords shall:

1. Be a minimum length of eight (8) characters on all systems.
2. Not be a dictionary word or proper name.
3. Not be the same as the Userid.
4. Expire within a maximum of 90 calendar days.
5. Not be identical to the previous ten (10) passwords.
6. Not be transmitted in the clear outside the secure location.
7. Not be displayed when entered.

5.6.2.1.1.2 Advanced Password Standards

When agencies elect to follow the advanced password standards, passwords shall:

1. Passwords shall be a minimum of twenty (20) characters in length with no additional complexity requirements imposed (e.g., ASCII characters, emojis, all keyboard characters, and spaces will be acceptable).
2. Password Verifiers shall not permit the use of a stored "hint" for forgotten passwords and/or prompt subscribers to use specific types of information (e.g., "What was the name of your first pet?") when choosing a password.
3. Verifiers shall maintain a list of "banned passwords" that contains values known to be commonly-used, expected, or compromised. For example, the list may include, but is not limited to:

- a. Passwords obtained from previous breach corpuses
 - b. Dictionary words
 - c. Repetitive or sequential characters (e.g. ‘aaaaaa’, ‘1234abcd’)
 - d. Context-specific words, such as the name of the service, the username, and derivatives thereof
4. When processing requests to establish and change passwords, Verifiers shall compare the prospective passwords against the “banned passwords” list.
 5. If the chosen password is found to be part of a “banned passwords” list, the Verifier shall:
 - a. Advise the subscriber that they need to select a different password,
 - b. Provide the reason for rejection, and
 - c. Require the subscriber to choose a different password.
 6. Verifiers shall limit the number of failed authentication attempts that can be made as described in Section 5.5.3 Unsuccessful Login Attempts.
 7. Verifiers shall force a password change if there is evidence of authenticator compromise or every 365 days from the last password change.
 8. Verifiers shall use approved encryption and an authenticated protected channel when requesting passwords to protect against eavesdropping and Man-in-the-Middle (MitM) attacks.
 9. Verifiers shall store passwords in a manner that is resistant to offline attacks by salting and hashing the password using a one-way key derivation function when stored.
 - a. The salt shall be at least 32 bits in length.
 - b. The salt shall be chosen arbitrarily so as to minimize salt value collisions among stored hashes.

Note: Key derivation functions take a password, a salt, and a cost factor as inputs then generate a password hash. Their purpose is to make each password guessing trial by an attacker who has obtained a password hash file expensive and therefore the cost of a guessing attack high or prohibitive.
 10. For each subscriber, Verifiers shall protect stored salt and resulting hash values using a password or PIN.

5.6.2.1.2 Personal Identification Number (PIN)

When agencies implement the use of a PIN as a standard authenticator, the PIN attributes shall follow the guidance in section 5.6.2.1.1 (password). When agencies utilize a PIN in conjunction with a certificate or a token (e.g. key fob with rolling numbers) for the purpose of advanced authentication, agencies shall follow the PIN attributes described below. For example: A user certificate is installed on a smartphone for the purpose of advanced authentication (AA). As the user invokes that certificate, a PIN meeting the below attributes shall be used to access the certificate for the AA process.

1. Be a minimum of six (6) digits
2. Have no repeating digits (i.e., 112233)
3. Have no sequential patterns (i.e., 123456)
4. Not be the same as the Userid.
5. Expire within a maximum of 365 calendar days.
 - a. If a PIN is used to access a soft certificate which is the second factor of authentication, AND the first factor is a password that complies with the requirements in Section 5.6.2.1.1, then the 365 day expiration requirement can be waived by the CSO.
6. Not be identical to the previous three (3) PINs.
7. Not be transmitted in the clear outside the secure location.
8. Not be displayed when entered.

EXCEPTION: When a PIN is used for local device authentication, the only requirement is that it be a minimum of six (6) digits.

5.6.2.1.3 One-time Passwords (OTP)

One-time passwords are considered a “something you have” token for authentication. Examples include bingo cards, hard or soft tokens, and out-of-band tokens (i.e. OTP received via a text message).

When agencies implement the use of an OTP as an authenticator, the OTP shall meet the requirements described below.

1. Be a minimum of six (6) randomly generated characters
2. Be valid for a single session
3. If not used, expire within a maximum of five (5) minutes after issuance

5.6.2.2 Advanced Authentication

Advanced Authentication (AA) provides for additional security to the typical user identification and authentication of login ID and password, such as: biometric systems, user-based digital certificates (e.g. public key infrastructure (PKI)), smart cards, software tokens, hardware tokens, paper (inert) tokens, out-of-band authenticators (retrieved via a separate communication service channel – e.g., authenticator is sent on demand via text message, phone call, etc.), or “Risk-based Authentication” that includes a software token element comprised of a number of factors, such as

network information, user information, positive device identification (i.e. device forensics, user pattern analysis and user binding), user profiling, and high-risk challenge/response questions.

When user-based certificates are used for authentication purposes, they shall:

1. Be specific to an individual user and not to a particular device.
2. Prohibit multiple users from utilizing the same certificate.
3. Require the user to “activate” that certificate for each use in some manner (e.g., passphrase or user-specific PIN).

5.6.2.2.1 Advanced Authentication Policy and Rationale

The requirement to use or not use AA is dependent upon the physical, personnel, and technical security controls associated with the user location and whether CJI is accessed directly or indirectly. AA shall not be required for users requesting access to CJI from within the perimeter of a physically secure location (Section 5.9), when the technical security controls have been met (Sections 5.5 and 5.10), or when the user has no ability to conduct transactional activities on state and national repositories, applications, or services (i.e. indirect access). Conversely, if the technical security controls have not been met, AA shall be required even if the request for CJI originates from within a physically secure location. Section 5.6.2.2.2 provides agencies with a decision tree to help guide AA decisions. The CSO will make the final determination of whether access is considered indirect.

The intent of AA is to meet the standards of two-factor authentication. Two-factor authentication employs the use of two of the following three factors of authentication: something you know (e.g. password), something you have (e.g. hard token), something you are (e.g. biometric). The two authentication factors shall be unique (i.e. password/token or biometric/password but not password/password or token/token).

EXCEPTION:

AA shall be required when the requested service has built AA into its processes and requires a user to provide AA before granting access. **EXAMPLES:**

1. A user, irrespective of his/her location, accesses the LEEP portal. The LEEP has AA built into its services and requires AA prior to granting access. AA is required.
2. A user, irrespective of their location, accesses a State’s portal through which access to CJI is facilitated. The State Portal has AA built into its processes and requires AA prior to granting access. AA is required.

5.6.2.2.2 Advanced Authentication Decision Tree

The following AA Decision Tree, coupled with figures 9 and 10 below, assists decision makers in determining whether or not AA is required.

1. Is the access to CJI direct access or indirect access?
 - a. If access is direct, proceed to question 2.
 - b. If access is indirect, decision tree is completed. AA is not required.
2. Can request’s physical originating location be determined?

If either (a) or (b) below are true the answer to the above question is “yes”. Proceed to question 3.

- a. The IP address is attributed to a physical structure; or
- b. The mnemonic is attributed to a specific device assigned to a specific location that is a physical structure.

If neither (a) or (b) above are true then the answer is “no”. Skip to question number 5.

3. Does request originate from within a physically secure location as described in Section 5.9.1?

If either (a) or (b) below are true the answer to the above question is “yes”. Proceed to question 4.

- a. The IP address is attributed to a physically secure location; or
- b. If a mnemonic is used it is attributed to a specific device assigned to a specific physically secure location.

If neither (a) or (b) above are true then the answer is “no”. Decision tree completed. AA required.

4. Are all required technical controls implemented at this location or at the controlling agency?

If either (a) or (b) below are true the answer to the above question is “yes”. Decision tree completed. AA is not required.

- a. Appropriate technical controls listed in Sections 5.5 and 5.10 are implemented; or
- b. The controlling agency (i.e. parent agency or agency leveraged as conduit to CJI) extends its wide area network controls down to the requesting agency and the extended controls provide assurance equal or greater to the controls listed in Sections 5.5 and 5.10.

If neither (a) or (b) above are true then the answer is “no”. Decision tree completed. AA required.

5. Does request originate from an agency-controlled user device?

If either (a) or (b) below are true the answer to the above question is “yes”. Proceed to question 6.

- a. The static IP address or MAC address can be traced to registered device; or
- b. Certificates are issued to agency managed devices only and certificate exchange is allowed only between authentication server and agency issued devices.

If neither (a) or (b) above are true then the answer is “no”. Decision tree completed. AA required.

6. Is the agency managed user device associated with and located within a criminal justice conveyance?

If any of the (a), (b), or (c) statements below is true the answer to the above question is “yes”. Proceed to Figure 9 Step 4.

- a. The static IP address or MAC address is associated with a device associated with a criminal justice conveyance; or
- b. The certificate presented is associated with a device associated with a criminal justice conveyance; or
- c. The mnemonic presented is associated with a specific device assigned and that device is attributed to a criminal justice conveyance.

If none of the (a), (b), or (c) statements above are true then the answer is “no”. Proceed to question number 7.

7. Is the user device an agency-issued and controlled smartphone or tablet?

If both (a) and (b) below are true, the answer to the above question is “yes.” Proceed to question number 8.

- a. The law enforcement agency issued the device to an individual; and
- b. The device is subject to administrative management control of the issuing agency.

If either (a) or (b) above is false, then the answer is “no.” Decision tree completed. AA required.

8. Does the agency-issued smartphone or tablet have CSO-approved AA compensating controls implemented?

If (a) and (b) below are true, the answer to the above question is “yes.” Decision tree completed. AA is not required.

- a. An agency cannot meet a requirement due to legitimate technical or business constraints; and
- b. The CSO has given written approval permitting temporary AA compensating controls to be implemented in lieu of the required AA control measures.

If either (a) or (b) above is false then the answer is “no.” Decision tree completed. AA required.

5.6.3 Identifier and Authenticator Management

The agency shall establish identifier and authenticator management processes.

5.6.3.1 Identifier Management

In order to manage user identifiers, agencies shall:

1. Uniquely identify each user.
2. Verify the identity of each user.
3. Receive authorization to issue a user identifier from an appropriate agency official.
4. Issue the user identifier to the intended party.

5. Disable the user identifier after a specified period of inactivity.
6. Archive user identifiers.

5.6.3.2 Authenticator Management

In order to manage information system authenticators, agencies shall:

1. Define initial authenticator content.
2. Establish administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators.
3. Change default authenticators upon information system installation.
4. Change/refresh authenticators periodically.

Information system authenticators include, for example, tokens, user-based PKI certificates, biometrics, passwords, and key cards. Users shall take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and immediately reporting lost or compromised authenticators.

5.6.4 Assertions

Identity providers can be leveraged to identify individuals and assert the individual's identity to a service or to a trusted broker who will in-turn assert the identity to a service. Assertion mechanisms used to communicate the results of a remote authentication to other parties shall be:

1. Digitally signed by a trusted entity (e.g., the identity provider).
2. Obtained directly from a trusted entity (e.g. trusted broker) using a protocol where the trusted entity authenticates to the relying party using a secure protocol (e.g. transport layer security [TLS]) that cryptographically authenticates the verifier and protects the assertion.

Assertions generated by a verifier shall expire after 12 hours and shall not be accepted thereafter by the relying party.

Figure 8 – Advanced Authentication Use Cases

Use Case 1 - A Local Police Department Authentication Control Scenario

During the course of an investigation, a detective attempts to access Criminal Justice Information (CJI) from a hotel room using an agency issued mobile broadband card. To gain access, the detective first establishes the remote session via a secure virtual private network (VPN) tunnel (satisfying the requirement for encryption). Upon connecting to the agency network, the detective is challenged for a username (identification), password ("something you know"), and a one-time password OTP ("something you have") from a hardware token to satisfy the requirement for advanced authentication. Once the detective's credentials are validated, his identity is asserted by the infrastructure to all authorized applications needed to complete his queries.

Use Case 2 – Use of a Smart Card

A user is issued a smart card that is loaded with user-specific digital certificates from a terminal within a controlled area. The user selects an application that will provide access to Criminal Justice Information (CJI) then enters the proper username (identification) and password (“something you know”). Once prompted, the user connects the smart card (“something you have”) to the terminal. The user is prompted to enter a personal identification number (PIN) to unlock the smart card. Once unlocked, the smart card sends the certificates to the authentication management server at the local agency where the combined username, password, and digital user certificates are validated. The user has satisfied the requirement for AA and is granted access to CJI.

Use Case 3 – Out of Band One-Time-Password (OTP) – Mobile phone-based

Using an agency- issued laptop, a user connects to the agency network via an agency-issued mobile broadband card and an encrypted virtual private network (VPN) tunnel. As part of an on-going investigation, the user initiates an application that will permit access to Criminal Justice Information (CJI). The user is prompted to enter a username (identification) and a password (“something you know”). Once that has been completed, a text message containing a one-time password (OTP) is sent via text message (out of band) to the user’s agency-issued cell phone. The user is challenged via the CJI application for that OTP. The user enters the OTP (“something you have”) then the username, password, and OTP are validated. The user has satisfied the requirement for AA and is granted access to CJI.

Use Case 4 – Improper Use of a One-Time-Password (OTP) – Laptop

Using an agency- issued laptop, a user connects to the agency network via an agency-issued mobile broadband card and an encrypted virtual private network (VPN) tunnel. As part of an on-going investigation, the user initiates an application that will permit access to Criminal Justice Information (CJI). The user is prompted to enter a username (identification) and a password (“something you know”). Once that has been completed, a one-time password (OTP) is sent to the user’s agency-issued laptop (in band) via pop-up message. The user is challenged via the CJI application for that OTP; however, the delivery of the OTP to the device that is being used to access CJI (in band) defeats the purpose of the second factor. This method does not satisfy the requirement for AA, and therefore the user should not be granted access to CJI. See the below explanation:

This method of receiving the necessary OTP (in band) does not guarantee the authenticity of the user’s identity because anyone launching the CJI application and entering a valid username/password combination is presented the OTP via a pop-up which is intend to be the second factor of authentication. This method makes the application accessible to anyone with knowledge of the valid username and password. Potentially, this is no more secure than using only a single factor of authentication.

Use Case 5 – Risk-based Authentication (RBA) Implementation

A user has moved office locations and requires email access (containing Criminal Justice Information) via an Outlook Web Access (OWA) client utilizes a risk-based authentication (RBA) solution. The user launches the OWA client and is prompted to enter a username (identification) and a password (“something you know”). The RBA detects this computer has not previously been used by the user, is not listed under the user’s profile, and then presents high-risk challenge/response question(s) which the user is prompted to answer. Once the questions have been verified as correct, the user is authenticated and granted access to the email. Meanwhile, the RBA logs and collects a number of device forensic information and captures the user pattern analysis to update the user’s profile. The CJIS Security Policy requirements for RBA have been satisfied.

Use Case 6 – Improper Risk-based Authentication (RBA) Implementation

A user has moved office locations and requires access to email containing Criminal Justice Information (CJI) via an Outlook Web Access (OWA) client utilizing a risk-based authentication (RBA) solution. The user launches the OWA client and is prompted to enter a username (identification) and a password (“something you know”). The RBA detects this computer has not previously been used by the user and is not listed under the user’s profile. The user is prompted to answer high-risk challenge/response questions for verification and authorization to access to the email; however, if the second authentication factor is to answer additional questions presented every time the user logs on, then this solution is referred to as a knowledge-based authentic on (KBA) solution. A KBA solution does not satisfy the requirement for AA, and therefore the user should not be granted access to CJI.

See the below explanation:

A KBA solution is not a viable advanced authentication (AA) solution per the CJIS Security Policy (CSP). The KBA asks questions and compares the answers to those stored within the user’s profile. A KBA is neither a CSP compliant two factor authentication solution, nor does it meet the CSP criteria of a risk-based authentication (RBA) solution which logs and collects a number of device forensic information and captures the user pattern analysis to update the user’s profile. Using this collected data, the RBA presents challenge/response questions when changes to the user’s profile are noted versus every time the user logs in.

Use Case 7 – Advanced Authentication Compensating Controls on Agency-Issued Smartphones

An authorized user is issued a smartphone that is administratively managed by the agency-installed mobile device management (MDM) solution to ensure device compliance with the CJIS Security Policy. The user initiates an email client on the smartphone that contains emails with CJI. The email client challenges the user to enter a username (identification) and a password (one factor: something you know) which are forwarded to the local agency for authentication. The smartphone lacks the technical capability to challenge the user for a second factor of authentication. This email client is used across the state agency so access is a necessity for the user’s job functions.

An audit by the CSA identifies the agency's use of the agency smartphone as not compliant with AA requirements due to the authorized user authenticating with only one factor instead of the required two factors.

Subsequently, the agency performs a risk assessment of their smartphone authentication solution and document a legitimate technical constraint due to the lack of technical solutions for smartphone-based two-factor authentication. The risk assessment identifies the following compensating controls that, when combined with the authorized user authenticating to the local agency with their password, meet the intent of the AA requirement by providing a similar level of security:

1. Enhance smartphone policy to enable possession of the smartphone to be considered a factor of authentication (i.e. something you have). Require authorized users to treat the smartphone as a controlled device and protect it as they would a personal credit card or an issued firearm to ensure only they will be in possession of the device
2. Move the email client used to authenticate with the local agency inside an encrypted, password-protected secure container on the smartphone ensuring only the authorized user can access the email application to authenticate.

The agency submits an AA compensating controls request to the CSO outlining the technical constraint identified by the risk assessment, what compensating controls will be employed, and the desired duration of the compensating controls.

The CSO approves the agency's request and provides documentation of the approval to the agency to maintain for audit purposes. The agency enacts the compensating controls and informs agency personnel they are permitted to access CJI via the agency-issued smartphone.

Figure 9 – Authentication Decision for Known Location

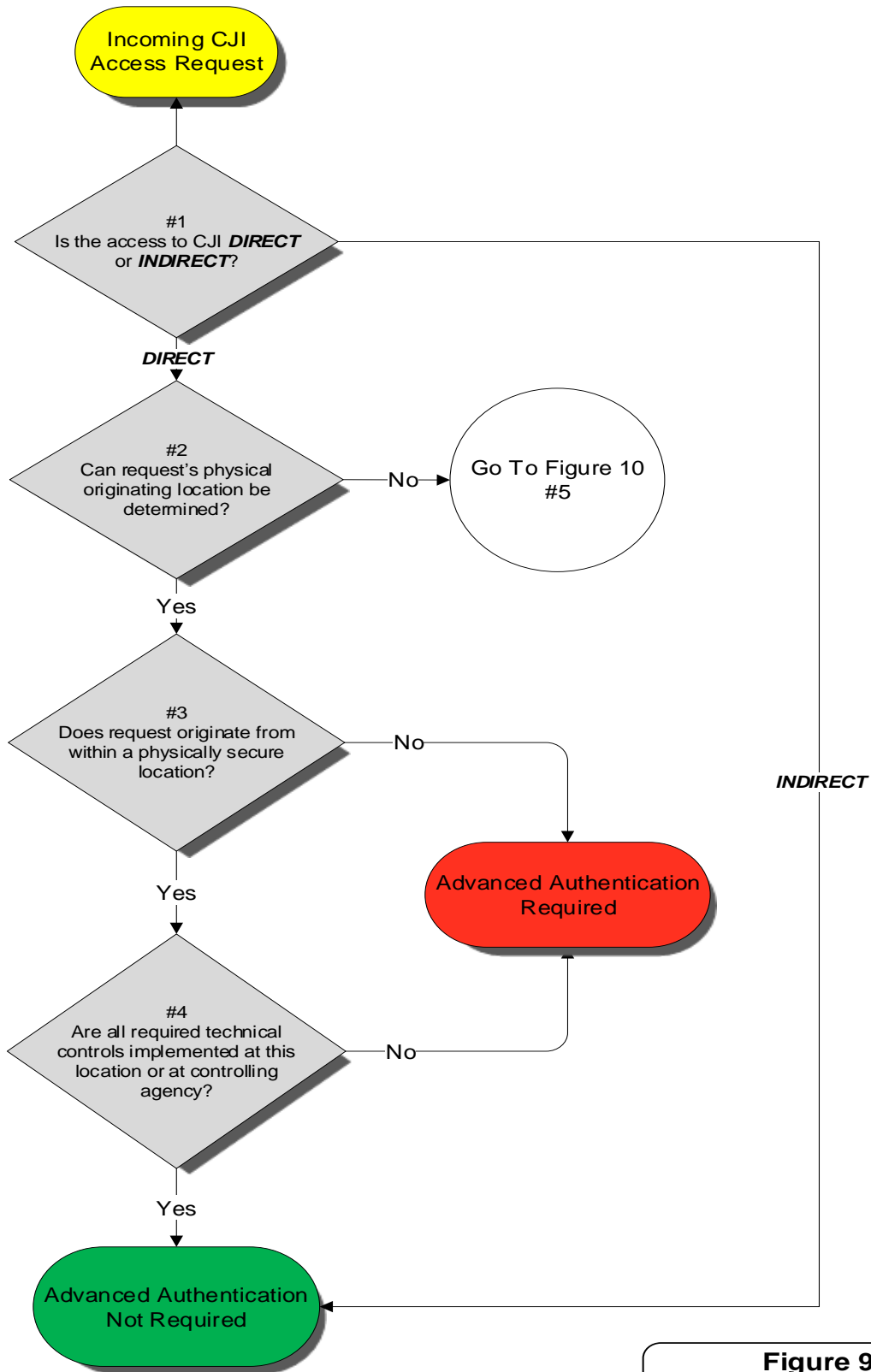


Figure 9		
	06/01/2020	

Figure 10 – Authentication Decision for Unknown Location

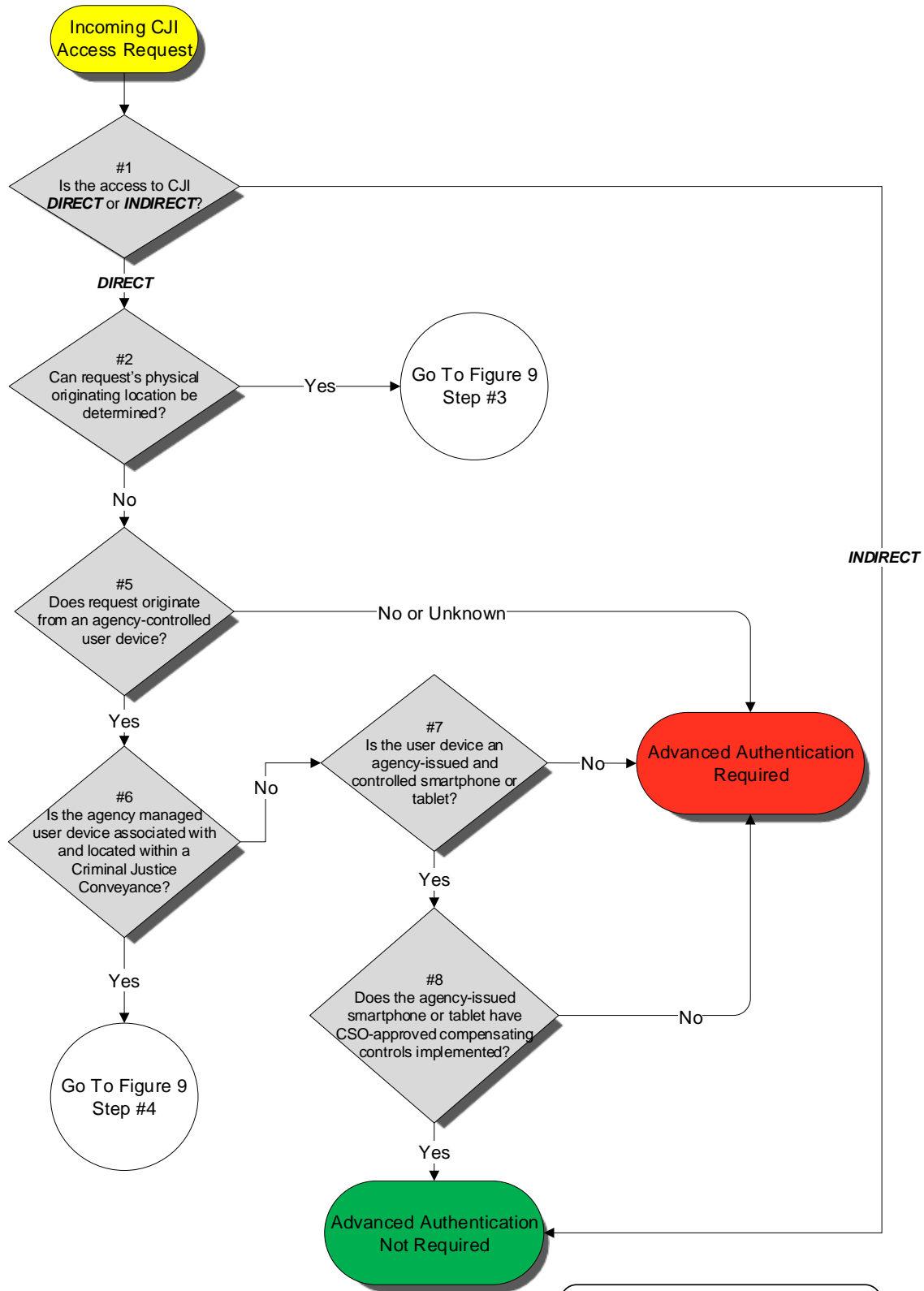


Figure 10		
	06/01/2020	

5.7 Policy Area 7: Configuration Management

5.7.1 Access Restrictions for Changes

Planned or unplanned changes to the hardware, software, and/or firmware components of the information system can have significant effects on the overall security of the system. The goal is to allow only qualified and authorized individuals access to information system components for purposes of initiating changes, including upgrades, and modifications. Section 5.5, Access Control, describes agency requirements for control of privileges and restrictions.

5.7.1.1 Least Functionality

The agency shall configure the application, service, or information system to provide only essential capabilities and shall specifically prohibit and/or restrict the use of specified functions, ports, protocols, and/or services.

5.7.1.2 Network Diagram

The agency shall ensure that a complete topological drawing depicting the interconnectivity of the agency network, to criminal justice information, systems and services is maintained in a current status. See Appendix C for sample network diagrams.

The network topological drawing shall include the following:

1. All communications paths, circuits, and other components used for the interconnection, beginning with the agency-owned system(s) and traversing through all interconnected systems to the agency end-point.
2. The logical location of all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations). Individual workstations (clients) do not have to be shown; the number of clients is sufficient.
3. “For Official Use Only” (FOUO) markings.
4. The agency name and date (day, month, and year) drawing was created or updated.

5.7.2 Security of Configuration Documentation

The system configuration documentation often contains sensitive details (e.g. descriptions of applications, processes, procedures, data structures, authorization processes, data flow, etc.) Agencies shall protect the system documentation from unauthorized access consistent with the provisions described in Section 5.5 Access Control.

Figure 11 – A Local Police Department’s Configuration Management Controls

A local police department decided to update their CAD system, and in doing so tracked all changes made to their infrastructure in a configuration management journal, updated their network topology documents to include all new components in their architecture, then marked all documentation as FOUO and stored them securely.

5.8 Policy Area 8: Media Protection

Media protection policy and procedures shall be documented and implemented to ensure that access to digital and physical media in all forms is restricted to authorized individuals. Procedures shall be defined for securely handling, transporting and storing media.

5.8.1 Media Storage and Access

The agency shall securely store digital and physical media within physically secure locations or controlled areas. The agency shall restrict access to digital and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data shall be encrypted per Section 5.10.1.2.

5.8.2 Media Transport

The agency shall protect and control digital and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.

5.8.2.1 Digital Media during Transport

Controls shall be in place to protect digital media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data. Encryption, as defined in Section 5.10.1.2 of this Policy, is the optimal control during transport; however, if encryption of the data isn't possible then each agency shall institute physical controls to ensure the security of the data.

5.8.2.2 Physical Media in Transit

The controls and security measures in this document also apply to CJI in physical (printed documents, printed imagery, etc.) form. Physical media shall be protected at the same level as the information would be protected in electronic form.

5.8.3 Digital Media Sanitization and Disposal

The agency shall sanitize, that is, overwrite at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.

5.8.4 Disposal of Physical Media

Physical media shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromise by unauthorized individuals. Physical media shall be destroyed by shredding or incineration. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.

Figure 12 – A Local Police Department’s Media Management Policies

A local police department implemented a replacement CAD system that integrated to their state’s CSA and was authorized to process CJI. The police department contracted with an off-site media manager to store backups of their data in the contractor’s vaults, but the contractor was not authorized to process or store CJI. To ensure the confidentiality of the police department’s data while outside its perimeter, they encrypted all data going to the contractor with an encryption product that is FIPS 140-2 certified. The police department rotated and reused media through the contractor’s vaults periodically, and when it required destruction, the police department incinerated the media to irreversibly destroy any data on it.

5.9 Policy Area 9: Physical Protection

Physical protection policy and procedures shall be documented and implemented to ensure CJI and information system hardware, software, and media are physically protected through access control measures.

5.9.1 Physically Secure Location

A physically secure location is a facility, a criminal justice conveyance, or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems. The physically secure location is subject to criminal justice agency management control; SIB control; FBI CJIS Security addendum; or a combination thereof.

Sections 5.9.1.1 – 5.9.1.8 describe the physical controls required in order to be considered a physically secure location, while Sections 5.2 and 5.12, respectively, describe the minimum security awareness training and personnel security controls required for unescorted access to a physically secure location. Sections 5.5, 5.6.2.2.1, and 5.10 describe the requirements for technical security controls required to access CJI from within the perimeter of a physically secure location without AA.

5.9.1.1 Security Perimeter

The perimeter of a physically secure location shall be prominently posted and separated from non-secure locations by physical controls. Security perimeters shall be defined, controlled and secured in a manner acceptable to the CSA or SIB.

5.9.1.2 Physical Access Authorizations

The agency shall develop and keep current a list of personnel with authorized access to the physically secure location (except for those areas within the permanent facility officially designated as publicly accessible) or shall issue credentials to authorized personnel.

5.9.1.3 Physical Access Control

The agency shall control all physical access points (except for those areas within the facility officially designated as publicly accessible) and shall verify individual access authorizations before granting access.

5.9.1.4 Access Control for Transmission Medium

The agency shall control physical access to information system distribution and transmission lines within the physically secure location.

5.9.1.5 Access Control for Display Medium

The agency shall control physical access to information system devices that display CJI and shall position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing CJI.

5.9.1.6 Monitoring Physical Access

The agency shall monitor physical access to the information system to detect and respond to physical security incidents.

5.9.1.7 Visitor Control

The agency shall control physical access by authenticating visitors before authorizing escorted access to the physically secure location (except for those areas designated as publicly accessible). The agency shall escort visitors at all times and monitor visitor activity.

5.9.1.8 Delivery and Removal

The agency shall authorize and control information system-related items entering and exiting the physically secure location.

5.9.2 Controlled Area

If an agency cannot meet all of the controls required for establishing a physically secure location, but has an operational need to access or store CJI, the agency shall designate an area, a room, or a storage container, as a controlled area for the purpose of day-to-day CJI access or storage. The agency shall, at a minimum:

1. Limit access to the controlled area during CJI processing times to only those personnel authorized by the agency to access or view CJI.
2. Lock the area, room, or storage container when unattended.
3. Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view.
4. Follow the encryption requirements found in Section 5.10.1.2 for electronic storage (i.e. data “at rest”) of CJI.

Figure 13 – A Local Police Department's Physical Protection Measures

A local police department implemented a replacement CAD system that was authorized to process CJI over an encrypted VPN tunnel to the state’s CSA. The police department established a physically separated wing within their precinct separated by locked doors, walls, and a monitored security system within which CJI was processed by criminal justice professionals. Only those persons with the appropriate authorizations were permitted within this wing unless accompanied by such a person. Within this secure wing the police department further segregated the back-office information systems’ infrastructure within a separately controlled area restricted only to those authorized administrative personnel with a need to enter.

5.10 Policy Area 10: System and Communications Protection and Information Integrity

Examples of systems and communications safeguards range from boundary and transmission protection to securing an agency's virtualized environment. In addition, applications, services, or information systems must have the capability to ensure system integrity through the detection and protection against unauthorized changes to software and information. This section details the policy for protecting systems and communications infrastructures.

Refer to Section 5.13.4 for additional system integrity requirements related to mobile devices used to access CJI.

5.10.1 Information Flow Enforcement

The network infrastructure shall control the flow of information between interconnected systems. Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. In other words, controlling how data moves from one place to the next in a secure manner. Examples of controls that are better expressed as flow control than access control (see Section 5.5) are:

1. Prevent CJI from being transmitted unencrypted across the public network.
2. Block outside traffic that claims to be from within the agency.
3. Do not pass any web requests to the public network that are not from the internal web proxy.

Specific examples of flow control enforcement can be found in boundary protection devices (e.g. proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services or provide a packet filtering capability.

5.10.1.1 Boundary Protection

The agency shall:

1. Control access to networks processing CJI.
2. Monitor and control communications at the external boundary of the information system and at key internal boundaries within the system.
3. Ensure any connections to the Internet, other external networks, or information systems occur through controlled interfaces (e.g. proxies, gateways, routers, firewalls, encrypted tunnels). See Section 5.13.4.3 for guidance on personal firewalls.
4. Employ tools and techniques to monitor network events, detect attacks, and provide identification of unauthorized use.
5. Ensure the operational failure of the boundary protection mechanisms do not result in any unauthorized release of information outside of the information system boundary (i.e. the device "fails closed" vs. "fails open").

6. Allocate publicly accessible information system components (e.g. public Web servers) to separate sub networks with separate, network interfaces. Publicly accessible information systems residing on a virtual host shall follow the guidance in Section 5.10.3.2 to achieve separation.

5.10.1.2 Encryption

Encryption is a form of cryptology that applies a cryptographic operation to provide confidentiality of (sensitive) information. Decryption is the reversing of the cryptographic operation to convert the information back into a plaintext (readable) format. There are two main types of encryption: symmetric encryption and asymmetric encryption (also known as public key encryption). Hybrid encryption solutions do exist and use both asymmetric encryption for client/server certificate exchange – session integrity and symmetric encryption for bulk data encryption – data confidentiality.

5.10.1.2.1 Encryption for CJI in Transit

When CJI is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via encryption. When encryption is employed, the cryptographic module used shall be FIPS 140-2 certified and use a symmetric cipher key strength of at least 128 bit strength to protect CJI.

NOTE: Subsequent versions of approved cryptographic modules that are under current review for FIPS 140-2 compliancy can be used in the interim until certification is complete.

EXCEPTIONS:

1. See Sections 5.13.1.2.2 and 5.10.2.
2. Encryption shall not be required if the transmission medium meets all of the following requirements:
 - a. The agency owns, operates, manages, or protects the medium.
 - b. Medium terminates within physically secure locations at both ends with no interconnections between.
 - c. Physical access to the medium is controlled by the agency using the requirements in Sections 5.9.1 and 5.12.
 - d. Protection includes safeguards (e.g., acoustic, electric, electromagnetic, and physical) and if feasible countermeasures (e.g., alarms, notifications) to permit its use for the transmission of unencrypted information through an area of lesser classification or control.
 - e. With prior approval of the CSO.

Examples:

- A campus is completely owned and controlled by a criminal justice agency (CJA)
 - If line-of-sight between buildings exists where a cable is buried, encryption is not required.

- A multi-story building is completely owned and controlled by a CJA – If floors are physically secure or cable runs through non-secure areas are protected, encryption is not required.
- A multi-story building is occupied by a mix of CJAs and non-CJAs – If floors are physically secure or cable runs through the non-secure areas are protected, encryption is not required.

5.10.1.2.2 Encryption for CJI at Rest

When CJI is at rest (i.e. stored digitally) outside the boundary of the physically secure location, the data shall be protected via encryption. When encryption is employed, agencies shall either encrypt CJI in accordance with the standard in Section 5.10.1.2.1 above, or use a symmetric cipher that is FIPS 197 certified (AES) and at least 256 bit strength.

1. When agencies implement encryption on CJI at rest, the passphrase used to unlock the cipher shall meet the following requirements:
 - a. Be at least 10 characters
 - b. Not be a dictionary word.
 - c. Include at least one (1) upper case letter, one (1) lower case letter, one (1) number, and one (1) special character.
 - d. Be changed when previously authorized personnel no longer require access.
2. Multiple files maintained in the same unencrypted folder shall have separate and distinct passphrases. A single passphrase may be used to encrypt an entire folder or disk containing multiple files. All audit requirements found in Section 5.4.1 Auditable Events and Content (Information Systems) shall be applied.

NOTE: Commonly available encryption tools often use a key to unlock the cipher to allow data access; this key is called a passphrase. While similar to a password, a passphrase is not used for user authentication. Additionally, the passphrase contains stringent character requirements making it more secure and thus providing a higher level of confidence that the passphrase will not be compromised.

5.10.1.2.3 Public Key Infrastructure (PKI) Technology

For agencies using public key infrastructure (PKI) technology, the agency shall develop and implement a certificate policy and certification practice statement for the issuance of public key certificates used in the information system. Registration to receive a public key certificate shall:

1. Include authorization by a supervisor or a responsible official.
2. Be accomplished by a secure process that verifies the identity of the certificate holder.
3. Ensure the certificate is issued to the intended party.

5.10.1.3 Intrusion Detection Tools and Techniques

Intrusion detection systems are deployed inside a network to monitor events against a known set of parameters (i.e. malicious activity or policy violations) and make notification to the system of any event which violates any of those parameters. They are passive in nature, listening and

monitoring network traffic. There are mainly two types of IDS; network-based IDS (NIDS) and host-based IDS (HIDS).

Intrusion prevention systems are an IDS with the capability to respond to detected intrusions. They are normally deployed at the perimeter of a network, scanning traffic. Like detection systems, protection systems compare scanned traffic to defined normal parameters but unlike detection systems are able to take some type of immediate action to mitigate, or prevent, an event.

Agencies shall:

1. Implement network-based and/or host-based intrusion detection or prevention tools.
2. Maintain current intrusion detection or prevention signatures.
3. Monitor inbound and outbound communications for unusual or unauthorized activities.
4. Send individual intrusion detection logs to a central logging facility where correlation and analysis will be accomplished as a system wide intrusion detection effort.
5. Review intrusion detection or prevention logs weekly or implement automated event notification.
6. Employ automated tools to support near-real-time analysis of events in support of detecting system-level attacks.

5.10.1.4 Voice over Internet Protocol

Voice over Internet Protocol (VoIP) has been embraced by organizations globally as an addition to, or replacement for, public switched telephone network (PSTN) and private branch exchange (PBX) telephone systems. The immediate benefits are lower costs than traditional telephone services and VoIP can be installed in-line with an organization's existing Internet Protocol (IP) services. Among VoIP's risks that have to be considered carefully are: myriad security concerns, cost issues associated with new networking hardware requirements, and overarching quality of service (QoS) factors.

In addition to the security controls described in this document, the following additional controls shall be implemented when an agency deploys VoIP within a network that contains unencrypted CJI:

1. Establish usage restrictions and implementation guidance for VoIP technologies.
2. Change the default administrative password on the IP phones and VoIP switches.
3. Utilize Virtual Local Area Network (VLAN) technology to segment VoIP traffic from data traffic.

Appendix G.2 outlines threats, vulnerabilities, mitigations, and NIST best practices for VoIP.

5.10.1.5 Cloud Computing

Organizations transitioning to a cloud environment are presented unique opportunities and challenges (e.g., purported cost savings and increased efficiencies versus a loss of control over the data). Reviewing the cloud computing white paper (Appendix G.3), the cloud assessment located within the security policy resource center on FBI.gov, NIST Special Publications (800-144, 800-

145, and 800-146), as well as the cloud provider's policies and capabilities will enable organizations to make informed decisions on whether or not the cloud provider can offer service that maintains compliance with the requirements of the CJIS Security Policy.

The storage of CJI, regardless of encryption status, shall only be permitted in cloud environments (e.g. government or third-party/commercial datacenters, etc.) which reside within the physical boundaries of APB-member country (i.e. U.S., U.S. territories, Indian Tribes, and Canada) and legal authority of an APB-member agency (i.e. U.S. – federal/state/territory, Indian Tribe, or the Royal Canadian Mounted Police (RCMP)).

Note: This restriction does not apply to exchanges of CJI with foreign government agencies under international exchange agreements (i.e. the Preventing and Combating Serious Crime (PCSC) agreements, fugitive extracts, and exchanges made for humanitarian and criminal investigatory purposes in particular circumstances).

Metadata derived from unencrypted CJI shall be protected in the same manner as CJI and shall not be used for any advertising or other commercial purposes by any cloud service provider or other associated entity.

The agency may permit limited use of metadata derived from unencrypted CJI when specifically approved by the agency and its "intended use" is detailed within the service agreement. Such authorized uses of metadata may include, but are not limited to the following: spam and spyware filtering, data loss prevention, spillage reporting, transaction logs (events and content – similar to Section 5.4), data usage/indexing metrics, and diagnostic/syslog data.

5.10.2 Facsimile Transmission of CJI

CJI transmitted via a single or multi-function device over a standard telephone line is exempt from encryption requirements. CJI transmitted external to a physically secure location using a facsimile server, application or service which implements email-like technology, shall meet the encryption requirements for CJI in transit as defined in Section 5.10.

5.10.3 Partitioning and Virtualization

As resources grow scarce, agencies are increasing the centralization of applications, services, and system administration. Advanced software now provides the ability to create virtual machines that allows agencies to reduce the amount of hardware needed. Although the concepts of partitioning and virtualization have existed for a while, the need for securing the partitions and virtualized machines has evolved due to the increasing amount of distributed processing and federated information sources now available across the Internet.

5.10.3.1 Partitioning

The application, service, or information system shall separate user functionality (including user interface services) from information system management functionality.

The application, service, or information system shall physically or logically separate user interface services (e.g. public web pages) from information storage and management services (e.g. database management). Separation may be accomplished through the use of one or more of the following:

1. Different computers.

2. Different central processing units.
3. Different instances of the operating system.
4. Different network addresses.
5. Other methods approved by the FBI CJIS ISO.

5.10.3.2 Virtualization

Virtualization refers to a methodology of dividing the resources of a computer (hardware and software) into multiple execution environments. Virtualized environments are authorized for criminal justice and noncriminal justice activities. In addition to the security controls described in this Policy, the following additional controls shall be implemented in a virtual environment:

1. Isolate the host from the virtual machine. In other words, virtual machine users cannot access host files, firmware, etc.
2. Maintain audit logs for all virtual machines and hosts and store the logs outside the hosts' virtual environment.
3. Virtual Machines that are Internet facing (web servers, portal servers, etc.) shall be physically separate from Virtual Machines (VMs) that process CJI internally or be separated by a virtual firewall.
4. Drivers that serve critical functions shall be stored within the specific VM they service. In other words, do not store these drivers within the hypervisor, or host operating system, for sharing. Each VM is to be treated as an independent system – secured as independently as possible.

The following additional technical security controls shall be applied in virtual environments where CJI is comingled with non-CJI:

1. Encrypt CJI when stored in a virtualized environment where CJI is comingled with non-CJI or segregate and store unencrypted CJI within its own secure VM.
2. Encrypt network traffic within the virtual environment.

The following are additional technical security control best practices and should be implemented wherever feasible:

1. Implement IDS and/or IPS monitoring within the virtual environment.
2. Virtually or physically firewall each VM within the virtual environment to ensure that only allowed protocols will transact.
3. Segregate the administrative duties for the host.

Appendix G-1 provides some reference and additional background information on virtualization.

5.10.4 System and Information Integrity Policy and Procedures

5.10.4.1 Patch Management

The agency shall identify applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws.

The agency (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) shall develop and implement a local policy that ensures prompt installation of newly released security relevant patches, service packs and hot fixes. Local policies should include such items as:

1. Testing of appropriate patches before installation.
2. Rollback capabilities when installing patches, updates, etc.
3. Automatic updates without individual user intervention.
4. Centralized patch management.

Patch requirements discovered during security assessments, continuous monitoring or incident response activities shall also be addressed expeditiously.

5.10.4.2 Malicious Code Protection

The agency shall implement malicious code protection that includes automatic updates for all systems with Internet access. Agencies with systems not connected to the Internet shall implement local procedures to ensure malicious code protection is kept current (i.e. most recent update available).

The agency shall employ virus protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses) at critical points throughout the network and on all workstations, servers and mobile computing devices on the network. The agency shall ensure malicious code protection is enabled on all of the aforementioned critical points and information systems and resident scanning is employed.

5.10.4.3 Spam and Spyware Protection

The agency shall implement spam and spyware protection.

The agency shall:

1. Employ spam protection mechanisms at critical information system entry points (e.g. firewalls, electronic mail servers, remote-access servers).
2. Employ spyware protection at workstations, servers and mobile computing devices on the network.
3. Use the spam and spyware protection mechanisms to detect and take appropriate action on unsolicited messages and spyware/adware, respectively, transported by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g. diskettes or compact disks) or other removable media as defined in this Policy.

5.10.4.4 Security Alerts and Advisories

The agency shall:

1. Receive information system security alerts/advisories on a regular basis.
2. Issue alerts/advisories to appropriate personnel.
3. Document the types of actions to be taken in response to security alerts/advisories.
4. Take appropriate actions in response.

5. Employ automated mechanisms to make security alert and advisory information available throughout the agency as appropriate.

5.10.4.5 Information Input Restrictions

The agency shall restrict the information input to any connection to FBI CJIS services to authorized personnel only.

Restrictions on personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities.

Figure 14 – System and Communications Protection and Information Integrity Use Cases

Use Case 1 – A Local Police Department’s Information Systems & Communications Protections

A local police department implemented a replacement CAD system within a physically secure location that was authorized to process CJI using a FIPS 140-2 encrypted VPN tunnel over the Internet to the state’s CSA. In addition to the policies, physical and personnel controls already in place, the police department employed firewalls both at their border and at key points within their network, intrusion detection systems, a patch-management strategy that included automatic patch updates where possible, virus scanners, spam and spyware detection mechanisms that update signatures automatically, and subscribed to various security alert mailing lists and addressed vulnerabilities raised through the alerts as needed.

Use Case 2 – Faxing from a Single/Multi-function Device over a Traditional Telephone Line

A dispatcher from county A runs a NCIC query on an individual. The results are printed and then sent to an adjoining county using a single/multi-function device with facsimile capability. For faxing, the device is only connected to a traditional telephone line as is the device at the receiving county. Encryption of a document containing CJI is not required because the document travels over a traditional telephone line.

Use Case 3 – Faxing from a Multi-function Device over a Network

A dispatcher from city A runs a NCIC query on an individual. The results are printed and the dispatcher uses a multi-function copier to fax the file to a city in another state. The dispatcher enters the fax number of the receiver and sends the document. The document containing CJI is automatically converted to a digital file and routed to the receiver over the agency network and the Internet. Because the device uses a network and the Internet for transmitting documents containing CJI, encryption in transit using FIPS 140-2 certified 128 bit symmetric encryption is required.

5.11 Policy Area 11: Formal Audits

Formal audits are conducted to ensure compliance with applicable statutes, regulations and policies.

5.11.1 Audits by the FBI CJIS Division

5.11.1.1 Triennial Compliance Audits by the FBI CJIS Division

The FBI CJIS Division is authorized to conduct audits, once every three (3) years as a minimum, to assess agency compliance with applicable statutes, regulations and policies. The CJIS Audit Unit (CAU) shall conduct a triennial audit of each CSA in order to verify compliance with applicable statutes, regulations and policies. This audit shall include a sample of CJAs and, in coordination with the SIB, the NCJAs. Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with applicable statutes, regulations and policies. The FBI CJIS Division shall also have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

5.11.1.2 Triennial Security Audits by the FBI CJIS Division

The FBI CJIS Division is authorized to conduct security audits of the CSA and SIB networks and systems, once every three (3) years as a minimum, to assess agency compliance with the CJIS Security Policy. This audit shall include a sample of CJAs and NCJAs. Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with the CJIS Security Policy.

5.11.2 Audits by the CSA

Each CSA shall:

1. At a minimum, triennially audit all CJAs and NCJAs which have direct access to the state system in order to ensure compliance with applicable statutes, regulations and policies.
2. In coordination with the SIB, establish a process to periodically audit all NCJAs, with access to CJI, in order to ensure compliance with applicable statutes, regulations and policies.
3. Have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.
4. Have the authority, on behalf of another CSA, to conduct a CSP compliance audit of contractor facilities and provide the results to the requesting CSA. If a subsequent CSA requests an audit of the same contractor facility, the CSA may provide the results of the previous audit unless otherwise notified by the requesting CSA that a new audit be performed.

Note: This authority does not apply to the audit requirement outlined in the Security and Management Control Outsourcing Standard for Non-Channeler and Channelers related to outsourcing noncriminal justice administrative functions.

5.11.3 Special Security Inquiries and Audits

All agencies having access to CJIS shall permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations. The inspection team shall be appointed by the APB and shall include at least one representative of the CJIS Division. All results of the inquiry and audit shall be reported to the APB with appropriate recommendations.

5.11.4 Compliance Subcommittees

The Criminal Justice Information Services (CJIS) Advisory Policy Board (APB) established the Compliance Evaluation Subcommittee (CES) to evaluate the results of audits conducted by the CJIS Audit Unit (CAU). The CES makes specific recommendations to the APB concerning compliance with applicable policies and regulations. The most current information regarding the CAU audits that are within the purview of the CES and detailed CES sanctions process procedures are available at CJIS.gov (Law Enforcement Enterprise Portal) CJIS Special Interest Groups CES Section and CJIS Section of FBI.gov.

The National Crime Prevention and Privacy Compact (Compact) Council at Article VI established the Compact Council (Council). The Compact Council Sanctions Committee is responsible for ensuring the use of the Interstate Identification Index System for noncriminal justice purposes complies with the Compact and with rules, standards, and procedures established by the Compact Council. As such, the Sanctions Committee reviews the results of audits conducted by the Federal Bureau of Investigation (FBI) of participants in the FBI's Criminal Justice Services (CJIS) Division programs. The Sanctions Committee reviews the audit results and the participant's response to determine a course of action necessary to bring the participant into compliance and make recommendations to the Compact Council or the FBI. Additional information on the Compact Council Sanctions process is available on the Compact Council's web-site.

Figure 15 – The Audit of a Local Police Department

A local police department implemented a replacement CAD system that integrated to their state's CSA and was authorized to process CJI. Shortly after the implementation, their state's CSA conducted an audit of their policies, procedures, and systems that process CJI. The police department supplied all architectural and policy documentation, including detailed network diagrams, to the auditors in order to assist them in the evaluation. The auditors discovered a deficiency in the police department's systems and marked them "out" in this aspect of the FBI CJIS Security Policy. The police department quickly addressed the deficiency and took corrective action, notifying the auditors of their actions.

5.12 Policy Area 12: Personnel Security

Having proper security measures against the insider threat is a critical component for the CJIS Security Policy. This section's security terms and requirements apply to all personnel who have unescorted access to unencrypted CJI including those individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI.

5.12.1 Personnel Screening Requirements for Individuals Requiring Unescorted Access to Unencrypted CJI

1. To verify identification, state of residency and national fingerprint-based record checks shall be conducted prior to granting access to CJI for all personnel who have unescorted access to unencrypted CJI or unescorted access to physically secure locations or controlled areas (during times of CJI processing). However, if the person resides in a different state than that of the assigned agency, the agency shall conduct state (of the agency) and national fingerprint-based record checks and execute a NLETS CHRI IQ/FQ/AQ query using purpose code C, E, or J depending on the circumstances. When appropriate, the screening shall be consistent with:
 - a. 5 CFR 731.106; and/or
 - b. Office of Personnel Management policy, regulations, and guidance; and/or
 - c. agency policy, regulations, and guidance.

Federal entities bypassing state repositories in compliance with federal law may not be required to conduct a state fingerprint-based record check.

See Appendix J for applicable guidance regarding noncriminal justice agencies performing adjudication of civil fingerprint submissions.

2. All requests for access shall be made as specified by the CSO. The CSO, or their designee, is authorized to approve access to CJI. All CSO designees shall be from an authorized criminal justice agency.
3. If a record of any kind exists, access to CJI shall not be granted until the CSO or his/her designee reviews the matter to determine if access is appropriate.
 - a. If a felony conviction of any kind exists, the Interface Agency shall deny access to CJI. However, the Interface Agency may ask for a review by the CSO in extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance.
 - b. Applicants with a record of misdemeanor offense(s) may be granted access if the CSO, or his or her designee, determines the nature or severity of the misdemeanor offense(s) do not warrant disqualification. The Interface Agency may request the CSO review a denial of access determination. This same procedure applies if the person is found to be a fugitive or has an arrest history without conviction.
 - c. If a record of any kind is found on a contractor, the CGA shall be formally notified and system access shall be delayed pending review of the criminal history record information. The CGA shall in turn notify the contractor's security officer.

4. If the person appears to be a fugitive or has an arrest history without conviction, the CSO or his/her designee shall review the matter to determine if access to CJI is appropriate.
5. If the person already has access to CJI and is subsequently arrested and or convicted, continued access to CJI shall be determined by the CSO. This does not implicitly grant hiring/firing authority with the CSA, only the authority to grant access to CJI. For offenses other than felonies, the CSO has the latitude to delegate continued access determinations to his or her designee.
6. If the CSO or his/her designee determines that access to CJI by the person would not be in the public interest, access shall be denied and the person's appointing authority shall be notified in writing of the access denial.
7. The granting agency shall maintain a list of personnel who have been authorized unescorted access to unencrypted CJI and shall, upon request, provide a current copy of the access list to the CSO.

It is recommended individual background re-investigations be conducted every five years unless Rap Back is implemented.

5.12.2 Personnel Termination

Upon termination of personnel by an interface agency, the agency shall immediately terminate access to local agency systems with access to CJI. Furthermore, the interface agency shall provide notification or other action to ensure access to state and other agency systems is terminated. If the employee is an employee of a NCJA or a Contractor, the employer shall notify all Interface Agencies that may be affected by the personnel change.

5.12.3 Personnel Transfer

The agency shall review CJI access authorizations when personnel are reassigned or transferred to other positions within the agency and initiate appropriate actions such as closing and establishing accounts and changing system access authorizations.

5.12.4 Personnel Sanctions

The agency shall employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.

Figure 16 – A Local Police Department's Personnel Security Controls

A local police department implemented a replacement CAD system that integrated to their state's CSA and was authorized to process CJI. In addition to the physical and technical controls already in place, the police department implemented a variety of personnel security controls to reduce the insider threat. The police department used background screening consistent with the FBI CJIS Security Policy to vet those with unescorted access to areas in which CJI is processed, including the IT administrators employed by a contractor and all janitorial staff. The police department established sanctions against any vetted person found to be in violation of stated

policies. The police department re-evaluated each person's suitability for access to CJI every five years.

5.13 Policy Area 13: Mobile Devices

This policy area describes considerations and requirements for mobile devices including smartphones and tablets. Mobile devices are not limited to a single form factor or communications medium. The requirements in this section augment those in other areas of the Policy to address the gaps introduced by using mobile devices.

The agency shall: (i) establish usage restrictions and implementation guidance for mobile devices; and (ii) authorize, monitor, control wireless access to the information system. Wireless technologies, in the simplest sense, enable one or more devices to communicate without physical connections—without requiring network or peripheral cabling.

Appendix G provides reference material and additional information on mobile devices.

5.13.1 Wireless Communications Technologies

Examples of wireless communication technologies include, but are not limited to: 802.11, cellular, Bluetooth, satellite, microwave, and land mobile radio (LMR). Wireless technologies require at least the minimum security applied to wired technology and, based upon the specific technology or implementation, wireless technologies may require additional security controls as described below.

5.13.1.1 802.11 Wireless Protocols

Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) cryptographic algorithms, used by all pre-802.11i protocols, do not meet the requirements for FIPS 140-2 and shall not be used.

Agencies shall implement the following controls for all agency-managed wireless access points with access to an agency's network that processes unencrypted CJI:

1. Perform validation testing to ensure rogue APs (Access Points) do not exist in the 802.11 Wireless Local Area Network (WLAN) and to fully understand the wireless network security posture.
2. Maintain a complete inventory of all Access Points (APs) and 802.11 wireless devices.
3. Place APs in secured areas to prevent unauthorized physical access and user manipulation.
4. Test AP range boundaries to determine the precise extent of the wireless coverage and design the AP wireless coverage to limit the coverage area to only what is needed for operational purposes.
5. Enable user authentication and encryption mechanisms for the management interface of the AP.
6. Ensure that all APs have strong administrative passwords and ensure that all passwords are changed in accordance with Section 5.6.2.1.
7. Ensure the reset function on APs is used only when needed and is only invoked by authorized personnel. Restore the APs to the latest security settings, when the reset functions are used, to ensure the factory default settings are not utilized.

8. Change the default service set identifier (SSID) in the APs. Disable the broadcast SSID feature so that the client SSID must match that of the AP. Validate that the SSID character string does not contain any agency identifiable information (division, department, street, etc.) or services.
9. Enable all security features of the wireless product, including the cryptographic authentication, firewall, and other available privacy features.
10. Ensure that encryption key sizes are at least 128-bits and the default shared keys are replaced by unique keys.
11. Ensure that the ad hoc mode has been disabled.
12. Disable all nonessential management protocols on the APs.
13. Ensure all management access and authentication occurs via FIPS compliant secure protocols (e.g. SFTP, HTTPS, SNMP over TLS, etc.). Disable non-FIPS compliant secure access to the management interface.
14. Enable logging (if supported) and review the logs on a recurring basis per local policy. At a minimum logs shall be reviewed monthly.
15. Insulate, virtually (e.g. virtual local area network (VLAN) and ACLs) or physically (e.g. firewalls), the wireless network from the operational wired infrastructure. Limit access between wireless networks and the wired network to only operational needs.
16. When disposing of access points that will no longer be used by the agency, clear access point configuration to prevent disclosure of network configuration, keys, passwords, etc.

5.13.1.2 Cellular Devices

Cellular telephones, smartphones (i.e. Blackberry, iPhones, etc.), tablets, personal digital assistants (PDA), and “aircards” are examples of cellular handheld devices or devices that are capable of employing cellular technology. Additionally, cellular handheld devices typically include Bluetooth, infrared, and other wireless protocols capable of joining infrastructure networks or creating dynamic ad hoc networks.

Threats to cellular handheld devices stem mainly from their size, portability, and available wireless interfaces and associated services. Examples of threats to cellular handheld devices include:

1. Loss, theft, or disposal.
2. Unauthorized access.
3. Malware.
4. Spam.
5. Electronic eavesdropping.
6. Electronic tracking (threat to security of data and safety of the criminal justice professional).
7. Cloning (not as prevalent with later generation cellular technologies).
8. Server-resident data.

5.13.1.2.1 Cellular Service Abroad

Certain internal functions on cellular devices may be modified or compromised by the cellular carrier during international use as the devices are intended to have certain parameters configured by the cellular provider which is considered a “trusted” entity by the device.

When devices are authorized to access CJI outside the U.S., agencies shall perform an inspection to ensure that all controls are in place and functioning properly in accordance with the agency’s policies prior to and after deployment outside of the U.S.

5.13.1.2.2 Voice Transmissions Over Cellular Devices

Any cellular device used to transmit CJI via voice is exempt from the encryption and authentication requirements.

5.13.1.3 Bluetooth

Bluetooth is an open standard for short-range radio frequency (RF) communication. Bluetooth is used primarily to establish wireless personal area networks (WPAN). Bluetooth technology has been integrated into many types of business and consumer devices, including cell phones, laptops, automobiles, medical devices, printers, keyboards, mice, headsets, and biometric capture devices.

Bluetooth technology and associated devices are susceptible to general wireless networking threats (e.g. denial of service [DoS] attacks, eavesdropping, man-in-the-middle [MITM] attacks, message modification, and resource misappropriation) as well as specific Bluetooth-related attacks that target known vulnerabilities in Bluetooth implementations and specifications. Organizational security policy shall be used to dictate the use of Bluetooth and its associated devices based on the agency’s operational and business processes.

5.13.1.4 Mobile Hotspots

Many mobile devices include the capability to function as a WiFi hotspot that allows other devices to connect through the device to the internet over the devices cellular network.

When an agency allows mobile devices that are approved to access or store CJI to function as a Wi-Fi hotspot connecting to the Internet, they shall be configured:

1. Enable encryption on the hotspot
2. Change the hotspot’s default SSID
 - a. Ensure the hotspot SSID does not identify the device make/model or agency ownership
3. Create a wireless network password (Pre-shared key)
4. Enable the hotspot’s port filtering/blocking features if present
5. Only allow connections from agency controlled devices

Note: Refer to the requirements in Section 5.10.1.2 encryption for item #1. Refer to the requirements in Section 5.6.2.2.1 Password for item #3. Only password attributes #1, #2 and #3 are required.

OR

1. Have a MDM solution to provide the same security as identified in items 1 – 5 above.

5.13.2 Mobile Device Management (MDM)

Mobile Device Management (MDM) facilitates the implementation of sound security controls for mobile devices and allows for centralized oversight of configuration control, application usage, and device protection and recovery, if so desired by the agency.

Due to the potential for inconsistent network access or monitoring capability on mobile devices, methods used to monitor and manage the configuration of full-featured operating systems may not function properly on devices with limited-feature operating systems. MDM systems and applications coupled with device specific technical policy can provide a robust method for device configuration management if properly implemented.

Devices that have had any unauthorized changes made to them (including but not limited to being rooted or jailbroken) shall not be used to process, store, or transmit CJI data at any time. User agencies shall implement the following controls when directly accessing CJI from devices running a limited-feature operating system:

1. Ensure that CJI is only transferred between CJI authorized applications and storage areas of the device.
2. MDM with centralized administration configured and implemented to perform at least the following controls:
 - a. Remote locking of device
 - b. Remote wiping of device
 - c. Setting and locking device configuration
 - d. Detection of “rooted” and “jailbroken” devices
 - e. Enforcement of folder or disk level encryption
 - f. Application of mandatory policy settings on the device
 - g. Detection of unauthorized configurations
 - h. Detection of unauthorized software or applications
 - i. Ability to determine the location of agency controlled devices
 - j. Prevention of unpatched devices from accessing CJI or CJI systems
 - k. Automatic device wiping after a specified number of failed access attempts

EXCEPTION: An MDM is not required when receiving CJI from an indirect access information system (i.e. the system provides no capability to conduct transactional activities on state and national repositories, applications or services). However, it is incumbent upon the authorized agency to ensure CJI is delivered to the appropriate requesting agency or individual. The CSO will make the final determination of whether access is considered indirect.

5.13.3 Wireless Device Risk Mitigations

Organizations shall, at a minimum, ensure that wireless devices:

1. Apply available critical patches and upgrades to the operating system as soon as they become available for the device and after necessary testing as described in Section 5.10.4.1.

2. Are configured for local device authentication (see Section 5.13.7.1).
3. Use advanced authentication or CSO approved compensating controls as per Section 5.13.7.2.1.
4. Encrypt all CJI resident on the device.
5. Erase cached information, to include authenticators (see Section 5.6.2.1) in applications, when session is terminated.
6. Employ personal firewalls on full-featured operating system devices or run a Mobile Device Management (MDM) system that facilitates the ability to provide firewall services from the agency level.
7. Employ malicious code protection on full-featured operating system devices or run a MDM system that facilitates the ability to provide anti-malware services from the agency level.

5.13.4 System Integrity

Managing system integrity on limited function mobile operating systems may require methods and technologies significantly different from traditional full-featured operating systems. In many cases, the requirements of Section 5.10 of the CJIS Security Policy cannot be met with a mobile device without the installation of a third party MDM, application, or supporting service infrastructure.

5.13.4.1 Patching/Updates

Based on the varying connection methods for mobile devices, an always on connection cannot be guaranteed for patching and updating. Devices without always-on cellular connections may not be reachable for extended periods of time by the MDM or solution either to report status or initiate patching.

Agencies shall monitor mobile devices to ensure their patch and update state is current.

5.13.4.2 Malicious Code Protection

Appropriately configured MDM software is capable of checking the installed applications on the device and reporting the software inventory to a central management console in a manner analogous to traditional virus scan detection of unauthorized software and can provide a high degree of confidence that only known software or applications are installed on the device.

Agencies that allow smartphones and tablets to access CJI shall have a process to approve the use of specific software or applications on the devices. Any device natively capable of performing these functions without a MDM solution is acceptable under this section.

5.13.4.3 Personal Firewall

For the purpose of this policy, a personal firewall is an application that controls network traffic to and from a user device, permitting or denying communications based on policy. A personal firewall shall be employed on all mobile devices that have a full-feature operating system (i.e. laptops or tablets with Windows or Linux/Unix operating systems). At a minimum, the personal firewall shall perform the following activities:

1. Manage program access to the Internet.

2. Block unsolicited requests to connect to the user device.
3. Filter incoming traffic by IP address or protocol.
4. Filter incoming traffic by destination ports.
5. Maintain an IP traffic log.

Mobile devices with limited-feature operating systems (i.e. tablets, smartphones) may not support a personal firewall. However, these operating systems have a limited number of system services installed, carefully controlled network access, and to a certain extent, perform functions similar to a personal firewall on a device with a full-feature operating system. Appropriately configured MDM software is capable of controlling which applications are allowed on the device.

5.13.5 Incident Response

In addition to the requirements in Section 5.3 Incident Response, agencies shall develop additional or enhanced incident reporting and handling procedures to address mobile device operating scenarios. Rapid response to mobile device related incidents can significantly mitigate the risks associated with illicit data access either on the device itself or within online data resources associated with the device through an application or specialized interface.

Special reporting procedures for mobile devices shall apply in any of the following situations:

1. Loss of device control. For example:
 - a. Device known to be locked, minimal duration of loss
 - b. Device lock state unknown, minimal duration of loss
 - c. Device lock state unknown, extended duration of loss
 - d. Device known to be unlocked, more than momentary duration of loss
2. Total loss of device
3. Device compromise
4. Device loss or compromise outside the United States

5.13.6 Access Control

Multiple user accounts are not generally supported on limited-feature mobile operating systems. Access control (Section 5.5 Access Control) shall be accomplished by the application that accesses CJI.

5.13.7 Identification and Authentication

Due to the technical methods used for identification and authentication on many limited-feature mobile operating systems, achieving compliance may require many different components.

5.13.7.1 Local Device Authentication

When mobile devices are authorized for use in accessing CJI, local device authentication shall be used to unlock the device for use. The authenticator used shall meet the requirements in section 5.6.2.1 Standard Authenticators.

5.13.7.2 Advanced Authentication

When accessing CJI from an authorized mobile device, advanced authentication shall be used by the authorized user unless the access to CJI is indirect as described in Section 5.6.2.2.1. If access is indirect, then AA is not required.

5.13.7.2.1 Compensating Controls

CSO approved compensating controls to meet the AA requirement on agency-issued smartphones and tablets with limited-feature operating systems are permitted. Compensating controls are temporary control measures that are implemented in lieu of the required AA control measures when an agency cannot meet a requirement due to legitimate technical or business constraints. Before CSOs consider approval of compensating controls, Mobile Device Management (MDM) shall be implemented per Section 5.13.2. The compensating controls shall:

1. Meet the intent of the CJIS Security Policy AA requirement
2. Provide a similar level of protection or security as the original AA requirement
3. Not rely upon the existing requirements for AA as compensating controls
4. Expire upon the CSO approved date or when a compliant AA solution is implemented.

Additionally, compensating controls may rely upon other, non-AA, existing requirements as compensating controls and/or be combined with new controls to create compensating controls.

The compensating controls for AA are a combination of controls providing acceptable assurance only the authorized user is authenticating and not an impersonator or (in the case of agency-issued device used by multiple users) controls that reduce the risk of exposure if information is accessed by an unauthorized party.

The following minimum controls shall be implemented as part of the CSO approved compensating controls:

- Possession and registration of an agency issued smartphone or tablet as an indication it is the authorized user
- Use of device certificates per Section 5.13.7.3 Device Certificates
- Implemented CJIS Security Policy compliant standard authenticator protection on the secure location where CJI is stored

5.13.7.3 Device Certificates

Device certificates are often used to uniquely identify mobile devices using part of a public key pair on the device in the form of a public key certificate. While there is value to ensuring the device itself can authenticate to a system supplying CJI, and may provide a critical layer of device identification or authentication in a larger scheme, a device certificate alone placed on the device shall not be considered valid proof that the device is being operated by an authorized user.

When certificates or cryptographic keys used to authenticate a mobile device are used in lieu of compensating controls for advanced authentication, they shall be:

1. Protected against being extracted from the device
2. Configured for remote wipe on demand or self-deletion based on a number of unsuccessful login or access attempts
3. Configured to use a secure authenticator (i.e. password, PIN) to unlock the key for use

APPENDICES

APPENDIX A TERMS AND DEFINITIONS

Access to Criminal Justice Information — The physical or logical (electronic) ability, right or privilege to view, modify or make use of Criminal Justice Information.

Administration of Criminal Justice — The detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. It also includes criminal identification activities; the collection, storage, and dissemination of criminal history record information; and criminal justice employment. In addition, administration of criminal justice includes “crime prevention programs” to the extent access to criminal history record information is limited to law enforcement agencies for law enforcement programs (e.g. record checks of individuals who participate in Neighborhood Watch or “safe house” programs) and the result of such checks will not be disseminated outside the law enforcement agency.

Agency Controlled Mobile Device — A mobile device that is centrally managed by an agency for the purpose of securing the device for potential access to CJJ. The device can be agency issued or BYOD (personally owned).

Agency Coordinator (AC) — A staff member of the Contracting Government Agency who manages the agreement between the Contractor and agency.

Agency Issued Mobile Device — A mobile device that is owned by an agency and issued to an individual for use. It is centrally managed by the agency for the purpose of securing the device for potential access to CJJ. The device is not BYOD (personally owned).

Agency Liaison (AL) — Coordinator of activities between the criminal justice agency and the noncriminal justice agency when responsibility for a criminal justice system has been delegated by a criminal justice agency to a noncriminal justice agency, which has in turn entered into an agreement with a contractor. The agency liaison shall, inter alia, monitor compliance with system security requirements. In instances in which the noncriminal justice agency's authority is directly from the CJIS systems agency, there is no requirement for the appointment of an agency liaison.

Asymmetric Encryption — A type of encryption that uses key pairs for encryption. One key is used to encrypt a message and another key to decrypt the message. Asymmetric encryption is also commonly known as public key encryption.

Authorized User/Personnel — An individual, or group of individuals, who have been appropriately vetted through a national fingerprint-based record check and have been granted access to CJJ.

Authorized Recipient — (1) A criminal justice agency or federal agency authorized to receive CHRI pursuant to federal statute or executive order; (2) A nongovernmental entity authorized by federal statute or executive order to receive CHRI for noncriminal justice purposes; or (3) A government agency authorized by federal statute or executive order, or state statute which has been approved by the United States Attorney General to receive CHRI for noncriminal justice purposes.

Availability — The degree to which information, a system, subsystem, or equipment is operable and in a useable state; frequently represented as a proportion of time the element is in a functioning condition.

Biographic Data — Information collected about individuals associated with a unique case, and not necessarily connected to identity data. Biographic Data does not provide a history of an individual, only information related to a unique case.

Biometric Data — When applied to CJI, it is used to identify individuals, and includes the following types: fingerprints, palm prints, DNA, iris, and facial recognition.

Case / Incident History — All relevant information gathered about an individual, organization, incident, or combination thereof, arranged so as to serve as an organized record to provide analytic value for a criminal justice organization. In regards to CJI, it is the information about the history of criminal incidents.

Certificate Authority (CA) Certificate – Digital certificates required for certificate-based authentication that are issued to tell the client computers and servers that it can trust other certificates that are issued by this CA.

Channeler — A FBI approved contractor, who has entered into an agreement with an Authorized Recipient(s), to receive noncriminal justice applicant fingerprint submissions and collect the associated fees. The Channeler ensures fingerprint submissions are properly and adequately completed, electronically forwards fingerprint submissions to the FBI's CJIS Division for national noncriminal justice criminal history record check, and receives electronic record check results for dissemination to Authorized Recipients. A Channeler is essentially an "expediter" rather than a user of criminal history record check results.

Cloud Client – A machine or software application that accesses cloud services over a network connection, perhaps on behalf of a subscriber.

Cloud Computing – A distributed computing model that permits on-demand network access to a shared pool of configurable computing resources (i.e., networks, servers, storage, applications, and services), software, and information.

Cloud Provider – An organization that provides cloud computing services.

Cloud Subscriber – A person or organization that is a customer of a cloud computing service provider.

CJIS Advisory Policy Board (APB) — The governing organization within the FBI CJIS Advisory Process composed of representatives from criminal justice and national security agencies within the United States. The APB reviews policy, technical, and operational issues relative to CJIS Division programs and makes subsequent recommendations to the Director of the FBI.

CJIS Audit Unit (CAU) — The organization within the FBI CJIS Division responsible to perform audits of CSAs to verify compliance with the CJIS Security Policy.

CJIS Security Policy — The FBI CJIS Security Policy document as published by the FBI CJIS ISO; the document containing this glossary.

CJIS Systems Agency (CSA) — A duly authorized state, federal, international, tribal, or territorial criminal justice agency on the CJIS network providing statewide (or equivalent) service to its criminal justice users with respect to the CJI from various systems managed by the FBI CJIS

Division. There shall be only one CSA per state or territory. In federal agencies, the CSA may be the interface or switch to other federal agencies connecting to the FBI CJIS systems.

CJIS Systems Agency Information Security Officer (CSA ISO) — The appointed FBI CJIS Division personnel responsible to coordinate information security efforts at all CJIS interface agencies.

CJIS Systems Officer (CSO) — The individual located within the CJIS Systems Agency responsible for the administration of the CJIS network on behalf of the CJIS Systems Agency.

Compact Council — The entity created by the National Crime Prevention and Privacy Compact of 1998 that has the authority to promulgate rules and procedures governing the use of the III system for noncriminal justice purposes.

Compact Officers — The leadership of the Compact Council, oversees the infrastructure established by the National Crime Prevention and Privacy Compact Act of 1998, which is used by ratifying states to exchange criminal records for noncriminal justice purposes. Their primary responsibilities are to promulgate rules and procedures for the effective and appropriate use of the III system.

Compensating Controls — Compensating controls are temporary control measures implemented in lieu of the required control measures when an agency cannot meet the AA requirement due to legitimate technical or business constraints. The compensating controls must:

1. Meet the intent of the CJIS Security Policy AA requirement
2. Provide a similar level of protection or security as the original AA requirement
3. Not rely upon the existing requirements for AA as compensating controls

Additionally, compensating controls may rely upon other, non-AA, existing requirements as compensating controls and/or be combined with new controls to create compensating controls.

Computer Security Incident Response Capability (CSIRC) — A collection of personnel, systems, and processes that are used to efficiently and quickly manage a centralized response to any sort of computer security incident which may occur.

Confidentiality — The concept of ensuring that information is observable only to those who have been granted authorization to do so.

Contractor — A private business, agency or individual which has entered into an agreement for the administration of criminal justice or noncriminal justice functions with a Criminal Justice Agency or a Noncriminal Justice Agency. Also, a private business approved by the FBI CJIS Division to contract with Noncriminal Justice Agencies to perform noncriminal justice functions associated with civil fingerprint submission for hiring purposes.

Contracting Government Agency (CGA) — The government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor.

Crime Reports Data — The data collected through the Uniform Crime Reporting program and reported upon annually by the FBI CJIS division used to analyze the crime statistics for the United States.

Criminal History Record Information (CHRI) — A subset of CJ. Any notations or other written or electronic evidence of an arrest, detention, complaint, indictment, information or other formal criminal charge relating to an identifiable person that includes identifying information regarding the individual as well as the disposition of any charges.

Criminal Justice Agency (CJA) — The courts, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspectors General Offices are included.

Criminal Justice Agency User Agreement — A terms-of-service agreement that must be signed prior to accessing CJ. This agreement is required by each CJA and spells out user's responsibilities, the forms and methods of acceptable use, penalties for their violation, disclaimers, and so on.

Criminal Justice Conveyance — A criminal justice conveyance is any enclosed mobile vehicle used for the purposes of criminal justice activities with the capability to comply, during operational periods, with the requirements of Section 5.9.1.3.

Criminal Justice Information (CJI) — Criminal Justice Information is the abstract term used to refer to all of the FBI CJIS provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to: biometric, identity history, person, organization, property (when accompanied by any personally identifiable information), and case/incident history data. In addition, CJI refers to the FBI CJIS-provided data necessary for civil agencies to perform their mission; including, but not limited to data used to make hiring decisions. The following type of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g. ORI, NIC, UCN, etc.) when not accompanied by information that reveals CJI or PII.

Criminal Justice Information Services Division (FBI CJIS or CJIS) — The FBI division responsible for the collection, warehousing, and timely dissemination of relevant CJI to the FBI and to qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies.

Data — See Information and CJI.

Decryption – The inverse cryptographic operation used to convert encrypted information back into a plaintext (readable) format.

Degauss — Neutralize a magnetic field to erase information from a magnetic disk or other storage device. In the field of information technology, degauss has become synonymous with erasing information whether or not the medium is magnetic. In the event the device to be degaussed is not magnetic (e.g. solid state drive, USB storage device), steps other than magnetic degaussing may be required to render the information irretrievable from the device.

Department of Justice (DoJ) — The Department within the U.S. Government responsible to enforce the law and defend the interests of the United States according to the law, to ensure public safety against threats foreign and domestic, to provide federal leadership in preventing and controlling crime, to seek just punishment for those guilty of unlawful behavior, and to ensure fair and impartial administration of justice for all Americans.

Digital Media – Any form of electronic media designed to store data in a digital format. This includes, but is not limited to: memory device in laptops, computers, and mobile devices; and any removable, transportable electronic media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card.

Digital Signature – A digital signature consists of three algorithms: (1) A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key. (2) A signing algorithm that, given a message and a private key, produces a signature. (3) A signature verifying algorithm that, given a message, public key, and a signature, either accepts or rejects the message’s claim to authenticity. Two main properties are required. First, a signature generated from a fixed message and fixed private key should verify the authenticity of that message by using the corresponding public key. Secondly, it should be computationally infeasible to generate a valid signature for a party who does not possess the private key.

Direct Access — (1) Having the authority to access systems managed by the FBI CJIS Division, whether by manual or automated methods, not requiring the assistance of, or intervention by, any other party or agency (28 CFR, Chapter 1, Part 20). (2) Having the authority to query or update national databases maintained by the FBI CJIS Division including national queries and updates automatically or manually generated by the CSA.

Dissemination — The transmission/distribution of CJIS to Authorized Recipients within an agency.

Encryption – A form of cryptology that applies a cryptographic operation to provide confidentiality of (sensitive) information.

Escort – Authorized personnel who accompany a visitor at all times while within a physically secure location to ensure the protection and integrity of the physically secure location and any Criminal Justice Information therein. The use of cameras or other electronic means used to monitor a physically secure location does not constitute an escort.

Facsimile (Fax) – Facsimile is: (a) a document received and printed on a single or multi-function stand-alone device, (b) a single or multi-function stand-alone device for the express purpose of transmitting and receiving documents from a like device over a standard telephone line, or (c) a facsimile server, application, service which implements email-like technology and transfers documents over a network.

Federal Bureau of Investigation (FBI) — The agency within the DOJ responsible to protect and defend the United States against terrorist and foreign intelligence threats, to uphold and enforce the criminal laws of the United States, and to provide leadership and criminal justice services to federal, state, municipal, and international agencies and partners.

FBI CJIS Information Security Officer (FBI CJIS ISO) — The FBI personnel responsible for the maintenance and dissemination of the FBI CJIS Security Policy; the liaison between the FBI and the CSA’s ISOs and other relevant security points-of-contact (POCs); the provider of technical guidance as to the intent and implementation of technical policy issues; the POC for computer incident notification which also disseminates security alerts to the CSOs and ISOs.

Federal Information Security Management Act (FISMA) — The Federal Information Security Management Act of 2002, a US Federal law that established information security standards for the protection of economic and national security interests of the United States. It requires each federal agency to develop, document, and implement an agency-wide program to provide information

security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

For Official Use Only (FOUO) — A caveat applied to unclassified sensitive information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA), 5 U.S.C 522. In general, information marked FOUO shall not be disclosed to anybody except Government (Federal, State, tribal, or local) employees or contractors with a need to know.

Full-feature Operating System — Full-feature operating systems are traditional operating systems used by a standard desktop computer (e.g. Microsoft Windows, Apple OSX/macOS, LINUX/UNIX, etc.). These operating systems are generally open to user control and configuration and therefore require configuration management to properly secure, or “harden”, these devices from malicious network based technical attacks (e.g. malware, spyware, hackers, etc.). These operating systems require traditional protection applications such as antivirus programs and personal firewalls.

Guest Operating System — An operating system that has emulated hardware presented to it by a host operating system. Also referred to as the virtual machine (VM).

Hashing — The process of applying a mathematical algorithm to data to produce an alphanumeric value (i.e. hash value) to be used as a representative of that data.

Hash Value — The term that refers to an alphanumeric value which represents the result of applying a cryptographic hash function to data.

Host Operating System — In the context of virtualization, the operating system that interfaces with the actual physical hardware and arbitrates between it and the guest operating systems. It is also referred to as a hypervisor.

Hybrid Encryption — A type of encryption where both asymmetric encryption and symmetric encryption keys are used creating what is referred to as cipher suites. In a hybrid solution the asymmetric encryption keys are used for client/server certificate exchange to provide session integrity while the symmetric encryption keys are used for bulk data encryption to provide data confidentiality.

Hypervisor — See Host Operating System.

Identity History Data — Textual data that corresponds with an individual’s biometric data, providing a history of criminal and/or civil events for the identified individual.

In-Band – The communication service channel (network connection, email, SMS text, phone call, etc.) used to obtain an authenticator is the same as the one used for login.

Indirect Access – Having the authority to access systems containing CJI without providing the user the ability to conduct transactional activities (the capability to query or update) on state and national systems (e.g. CJIS Systems Agency (CSA), State Identification Bureau (SIB), or national repositories).

Information — See data and CJI.

Information Exchange Agreement — An agreement that codifies the rules by which two parties engage in the sharing of information. These agreements typically include language which establishes some general duty-of-care over the other party’s information, whether and how it can be further disseminated, penalties for violations, the laws governing the agreement (which

establishes venue), procedures for the handling of shared information at the termination of the agreement, and so on. This document will ensure consistency with applicable federal laws, directives, policies, regulations, standards and guidance.

Information Security Officer (ISO) — Typically a member of an organization who has the responsibility to establish and maintain information security policy, assesses threats and vulnerabilities, performs risk and control assessments, oversees the governance of security operations, and establishes information security training and awareness programs. The ISO also usually interfaces with security operations to manage implementation details and with auditors to verify compliance to established policies.

Information System — A system of people, data, and processes, whether manual or automated, established for the purpose of managing information.

Integrated Automated Fingerprint Identification System (IAFIS) — The national fingerprint and criminal history system maintained by the FBI CJIS Division that provides the law enforcement community with automated fingerprint search capabilities, latent searching capability, electronic image storage, and electronic exchange of fingerprints and responses.

Integrity — The perceived consistency of expected outcomes, actions, values, and methods of an individual or organization. As it relates to data, it is the concept that data is preserved in a consistent and correct state for its intended use.

Interconnection Security Agreement (ISA) — An agreement much like an Information Exchange Agreement as mentioned above, but concentrating more on formalizing the technical and security requirements pertaining to some sort of interface between the parties' information systems.

Interface Agency — A legacy term used to describe agencies with direct connections to the CSA. This term is now used predominantly in a common way to describe any sub-agency of a CSA or SIB that leverages the CSA or SIB as a conduit to FBI CJIS information.

Internet Protocol (IP) — A protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP. IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses.

Interstate Identification Index (III) — The CJIS service that manages automated submission and requests for CHRI that is warehoused subsequent to the submission of fingerprint information. Subsequent requests are directed to the originating State as needed.

Intrusion Detection — The process of monitoring the events occurring in an information system or network and analyzing them for signs of possible incidents.

Intrusion Detection System — Software which automates the intrusion detection process.

Intrusion Prevention — The process of monitoring events occurring in an information system or network and analyzing them for signs of possible incidents and attempting to stop detected possible incidents.

Intrusion Prevention System — Software which has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents.

Jailbreak (Jailbroken) — The process of attaining privileged control (known as “root access”) of a device running the Apple iOS operating system that ultimately allows a user the ability to alter or replace system applications and settings, run specialized applications that require administrator-level permissions, or perform other operations that are otherwise not allowed.

Laptop Devices – Laptop devices are mobile devices with a full-featured operating system (e.g. Microsoft Windows, Apple OSX/macOS, LINUX/UNIX, etc.). Laptops are typically intended for transport via vehicle mount or portfolio-sized carry case, but not on the body. This definition does not include pocket/handheld devices (e.g. smartphones), or mobile devices that feature a limited-feature operating system (e.g. tablets).

Law Enforcement Enterprise Portal (LEEP) — A secure, Internet-based communications portal provided by the FBI CJIS Division for use by law enforcement, first responders, criminal justice professionals, and anti-terrorism and intelligence agencies around the globe. Its primary purpose is to provide a platform on which various law enforcement agencies can collaborate on FOUO matters.

Limited-feature Operating System — Limited-feature operating systems are designed specifically for the mobile environment where battery life and power efficiency are primary design drivers (e.g. Apple iOS, Android, Windows Mobile, Blackberry OS, etc.). These operating systems permit limited user control, but are inherently more resistant than a full-feature operating system to certain types of network based technical attacks due to the limited-feature sets. Devices using these operating systems are required to be managed by a mobile device management solution.

Logical Access – The technical means (e.g., read, create, modify, delete a file, execute a program, or use an external connection) for an individual or other computer system to utilize CJI or CJIS applications.

Logical Partitioning – When the host operating system, or hypervisor, allows multiple guest operating systems to share the same physical resources.

Local Agency Security Officer (LASO) — The primary Information Security contact between a local law enforcement agency and the CSA under which this agency interfaces with the FBI CJIS Division. The LASO actively represents their agency in all matters pertaining to Information Security, disseminates Information Security alerts and other material to their constituents, maintains Information Security documentation (including system configuration data), assists with Information Security audits of hardware and procedures, and keeps the CSA informed as to any Information Security needs and problems.

Management Control Agreement (MCA) — An agreement between parties that wish to share or pool resources that codifies precisely who has administrative control over, versus overall management and legal responsibility for, assets covered under the agreement. An MCA must ensure the CJA’s authority remains with regard to all aspects of Section 3.2.2. The MCA usually results in the CJA having ultimate authority over the CJI supporting infrastructure administered by the NCJA.

Metadata — Structured information that describes, explains, locates or otherwise makes it easier to retrieve, use or manage an information resource. Metadata is commonly referred to as data about data, information about information, or information describing the characteristics of data.

Mobile Device — Any portable device used to access CJI via a wireless connection (e.g. cellular, WiFi, Bluetooth, etc.).

Mobile Device Management (MDM) — Centralized administration and control of mobile devices specifically including, but not limited to, cellular phones, smart phones, and tablets. Management typically includes the ability to configure device settings and prevent a user from changing them, remotely locating a device in the event of theft or loss, and remotely locking or wiping a device. Management can also include over-the-air distribution of applications and updating installed applications.

Mobile (WiFi) Hotspot — A mobile (WiFi) hotspot is a zone or area associated with a mobile device (e.g. smartphone, air card) allowing wireless connectivity to the Internet typically through a cellular connection.

National Crime Information Center (NCIC) — An information system which stores CJJ which can be queried by appropriate Federal, state, and local law enforcement and other criminal justice agencies.

National Instant Criminal Background Check System (NICS) — A system mandated by the Brady Handgun Violence Prevention Act of 1993 that is used by Federal Firearms Licensees (FFLs) to instantly determine via telephone or other electronic means whether the transfer of a firearm would be in violation of Section 922 (g) or (n) of Title 18, United States Code, or state law, by evaluating the prospective buyer's criminal history.

National Institute of Standards and Technology (NIST) — Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Department of Commerce whose mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic and national security.

Noncriminal Justice Agency (NCJA) — A governmental agency, or any subunit thereof, that provides services primarily for purposes other than the administration of criminal justice. Examples of services include, but not limited to, employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

NCJA (Government) — A Federal, state, local, or tribal governmental agency or any subunit thereof whose charter does not include the responsibility to administer criminal justice, but may have a need to process CJJ. An example would be the central IT organization within a state government that administers equipment on behalf of a state law-enforcement agency.

NCJA (Private) — A private agency or subunit thereof whose charter does not include the responsibility to administer criminal justice, but may have a need to process CJJ. An example would include a local bank.

NCJA (Public) — A public agency or sub-unit thereof whose charter does not include the responsibility to administer criminal justice, but may have a need to process CJJ. An example would include a county school board which uses CHRI to assist in employee hiring decisions.

Noncriminal Justice Purpose — The uses of criminal history records for purposes authorized by federal or state law other than purposes relating to the administration of criminal justice, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

Office of Management and Budget (OMB) — The agency within the Executive Branch of the Federal government responsible to oversee the preparation of the federal budget, to assist in the

supervision of other Executive Branch agencies, and to oversee and coordinate the Presidential Administration's procurement, financial management, information, and regulatory policies.

One-time Password — A disposable, single-use standard authenticator for access CJI. One-time passwords are: minimum of six (6) randomly generated characters, valid for a single session, and if not used, expire within a minimum of five (5) minutes after issuance.

Out-of-Band — The communication service channel (network connection, email, SMS text, phone call, etc.) used to obtain an authenticator is separate from that used for login.

Outsourcing — The process of delegating in-house operations to a third-party. For instance, when the administration of criminal justice functions (network operations, dispatch functions, system administration operations, etc.) are performed for the criminal justice agency by a city or county information technology department or are contracted to be performed by a vendor.

Outsourcing Standard — National Crime Prevention and Privacy Compact Council's Outsourcing Standard. The Compact Council's uniform standards and processes for the interstate and Federal-State exchange of criminal history records for noncriminal justice purposes.

Partitioning – Managing guest operating system, or virtual machine, access to hardware so that each guest OS can access its own resources but cannot encroach on the other guest operating systems resources or any resources not allocated for virtualization use.

Password Verifier (Verifier) – An entity or process that verifies the claimant's identity by verifying the claimant's possession and control of one or two authenticators using an authentication protocol. To do this, the Verifier may also need to validate credentials that link the authenticator(s) to the subscriber's identifier and check their status.

Personal Firewall — An application which controls network traffic to and from a computer, permitting or denying communications based on a security policy.

Personally Identifiable Information (PII) — PII is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name.

Physical Access – The physical ability, right or privilege to view, modify or make use of Criminal Justice Information (CJI) by means of physical presence within the proximity of computers and network devices (e.g. the ability to insert a boot disk or other device into the system, make a physical connection with electronic equipment, etc.).

Physical Media – Physical media refers to media in printed form. This definition includes, but is not limited to, printed documents, printed imagery, printed facsimile.

Physical Partitioning – When the host operating system, or hypervisor, assigns separate physical resources to each guest operating systems, or virtual machine.

Physically Secure Location — A facility, a criminal justice conveyance, or an area, a room, or a group of rooms, within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems.

Pocket/Handheld Mobile Device – Pocket/Handheld mobile devices (e.g. smartphones) are intended to be carried in a pocket or holster attached to the body and feature an operating system

with limited functionality (e.g., iOS, Android, BlackBerry, etc.). This definition does not include tablet and laptop devices.

Property Data — Information about vehicles and property associated with a crime.

Rap Back — A NGI service that allows authorized agencies to receive notification of subsequent criminal activity reported to the FBI committed by persons of interest.

Receive-Only Terminal (ROT) – A device that is configured to accept a limited type of data but is technically prohibited from forming or transmitting data, browsing or navigating internal or external networks, or otherwise performing outside the scope of receive only (e.g., a printer, dumb terminal, etc.).

Repository Manager, or Chief Administrator — The designated manager of the agency having oversight responsibility for a CSA’s fingerprint identification services. If both state fingerprint identification services and CJIS systems control are managed within the same state agency, the repository manager and CSO may be the same person.

Root (Rooting, Rooted) — The process of attaining privileged control (known as “root access”) of a device running the Android operating system that ultimately allows a user the ability to alter or replace system applications and settings, run specialized applications that require administrator-level permissions, or perform other operations that are otherwise not allowed.

Salting –The process of applying a non-secret value to data prior to applying a cryptographic process, such as hashing. This process changes the value to be hashed in a manner designed to ensure an attacker cannot reuse the results of computations for one instance.

Secondary Dissemination — The promulgation of CJI from a releasing agency to an authorized recipient agency when the recipient agency has not been previously identified in a formal information exchange agreement.

Security Addendum (SA) — A uniform addendum to an agreement between the government agency and a private contractor, approved by the Attorney General of the United States, which specifically authorizes access to criminal history record information, limits the use of the information to the purposes for which it is provided, ensures the security and confidentiality of the information consistent with existing regulations and the CJIS Security Policy, provides for sanctions, and contains such other provisions as the Attorney General may require.

Sensitive But Unclassified (SBU) — Designation of information in the United States federal government that, though unclassified, often requires strict controls over its distribution. SBU is a broad category of information that includes material covered by such designations as For Official Use Only (FOUO), Law Enforcement Sensitive (LES), Sensitive Homeland Security Information, Security Sensitive Information (SSI), Critical Infrastructure Information (CII), etc. Some categories of SBU information have authority in statute or regulation (e.g. SSI, CII) while others, including FOUO, do not. As of May 9, 2008, the more appropriate terminology to use is Controlled Unclassified Information (CUI).

Server/Client Computer Certificate (device-based) – Digital certificates that are issued to servers or client computers or devices by a CA and used to prove device identity between server and/or client computer devices during the authentication process.

Service — The organized system of apparatus, appliances, personnel, etc, that supply some tangible benefit to the consumers of this service. In the context of CJI, this usually refers to one of the applications that can be used to process CJI.

Shredder — A device used for shredding documents, often as a security measure to prevent unapproved persons from reading them. Strip-cut shredders, also known as straight-cut or spaghetti-cut, slice the paper into long, thin strips but are not considered secure. Cross-cut shredders provide more security by cutting paper vertically and horizontally into confetti-like pieces.

Smartphone – See pocket/handheld mobile devices.

Social Engineering — The act of manipulating people into performing actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information gathering, fraud, or computer system access; in most cases the attacker never comes face-to-face with the victim.

Software Patch — A piece of software designed to fix problems with, or update, a computer program or its supporting data. This includes fixing security vulnerabilities and other bugs and improving the usability or performance. Though meant to fix problems, poorly designed patches can sometimes introduce new problems. As such, patches should be installed in a test environment prior to being installed in a live, operational system. Patches often can be found in multiple locations but should be retrieved only from sources agreed upon through organizational policy.

State and Federal Agency User Agreement — A written agreement that each CSA or SIB Chief shall execute with the FBI CJIS Division stating their willingness to demonstrate conformance with the FBI CJIS Security Policy prior to the establishment of connectivity between organizations. This agreement includes the standards and sanctions governing use of CJIS systems, as well as verbiage to allow the FBI to periodically audit the CSA as well as to allow the FBI to penetration test its own network from the CSA's interfaces to it.

State Compact Officer — The representative of a state that is party to the National Crime Prevention and Privacy Compact, and is the chief administrator of the state's criminal history record repository or a designee of the chief administrator who is a regular full-time employee of the repository.

State Identification Bureau (SIB) — The state agency with the responsibility for the state's fingerprint identification services.

State Identification Bureau (SIB) Chief — The SIB Chief is the designated manager of state's SIB. If both state fingerprint identification services and CJIS systems control are managed within the same state agency, the SIB Chief and CSO may be the same person.

State of Residency – A state of residency is the state in which an individual claims and can provide documented evidence as proof of being his/her permanent living domicile. CJIS Systems Officers have the latitude to determine what documentation constitutes acceptable proof of residency.

Symmetric Encryption — A type of encryption where the same key is used to encrypt and decrypt a message. Symmetric encryption is also known as secret key encryption.

System — Refer to connections to the FBI's criminal justice information repositories and the equipment used to establish said connections. In the context of CJI, this usually refers to

applications and all interconnecting infrastructure required to use those applications that process CJJ.

Tablet Devices – Tablet devices are mobile devices with a limited-feature operating system (e.g. iOS, Android, Windows RT, etc.). Tablets typically consist of a touch screen without a permanently attached keyboard intended for transport via vehicle mount or portfolio-sized carry case but not on the body. This definition does not include pocket/handheld devices (e.g. smartphones) or mobile devices with full-featured operating systems (e.g. laptops).

Terminal Agency Coordinator (TAC) — Serves as the point-of-contact at the local agency for matters relating to CJIS information access. A TAC administers CJIS systems programs within the local agency and oversees the agency's compliance with CJIS systems policies.

User Certificate (user-based) – Digital certificates that are unique and issued to individuals by a CA. Though not always required to do so, these specific certificates are often embedded on smart cards or other external devices as a means of distribution to specified users. This certificate is used when individuals need to prove their identity during the authentication process.

Virtual Escort – Authorized personnel who actively monitor a remote maintenance session on Criminal Justice Information (CJI)-processing systems. The escort must have the ability to end the session at any time deemed necessary to ensure the protection and integrity of CJI at all times.

Virtual Machine (VM) – See Guest Operating System

Virtualization — Refers to a methodology of dividing the resources of a computer (hardware and software) into multiple execution environments, by applying one or more concepts or technologies such as hardware and software partitioning, time-sharing, partial or complete machine simulation or emulation allowing multiple operating systems, or images, to run concurrently on the same hardware.

Voice over Internet Protocol (VoIP) — A set of software, hardware, and standards designed to make it possible to transmit voice over packet switched networks, either an internal Local Area Network, or across the Internet.

Wireless Access Point – A wireless access point is a device that logically connects a wireless client device to an organization's enterprise network which processes unencrypted CJJ.

Wireless (WiFi) Hotspot – A wireless (WiFi) hotspot is a zone or area within a fixed location allowing wireless connectivity to the Internet typically through a wired connection. Hotspots are typically available in public areas such as airports, hotels and restaurants.

APPENDIX B ACRONYMS

Acronym	Term
AA	Advanced Authentication
AC	Agency Coordinator
ACL	Access Control List
AES	Advanced Encryption Standard
AP	Access Point
APB	Advisory Policy Board
BD-ADDR	Bluetooth-Enabled Wireless Devices and Addresses
BYOD	Bring Your Own Device
CAD	Computer-Assisted Dispatch
CAU	CJIS Audit Unit
CFR	Code of Federal Regulations
CGA	Contracting Government Agency
CHRI	Criminal History Record Information
CJA	Criminal Justice Agency
CJI	Criminal Justice Information
CJIS	Criminal Justice Information Services
ConOps	Concept of Operations
CSA	CJIS Systems Agency
CSIRC	Computer Security Incident Response Capability
CSO	CJIS Systems Officer
DAA	Designated Approving Authority
DoJ	Department of Justice

DoJCERT	DoJ Computer Emergency Response Team
FBI	Federal Bureau of Investigation
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FOUO	For Official Use Only
HIDS	Host-based Intrusion Detection System
HIPS	Host-based Intrusion Prevention System
HTTP	Hypertext Transfer Protocol
IAFIS	Integrated Automated Fingerprint Identification System
IDS	Intrusion Detection System
III	Interstate Identification Index
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSEC	Internet Protocol Security
ISA	Interconnection Security Agreement
ISO	Information Security Officer
IT	Information Technology
LASO	Local Agency Security Officer
LEEP	Law Enforcement Enterprise Portal
LMR	Land Mobile Radio
MAC	Media Access Control
MCA	Management Control Agreement
MDM	Mobile Device Management
MITM	Man-in-the-Middle

MOU	Memorandum of Understanding
NCIC	National Crime Information Center
NCJA	Noncriminal Justice Agency
NICS	National Instant Criminal Background Check System
NIDS	Network-based Intrusion Detection System
NIPS	Network-based Intrusion Prevention System
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
ORI	Originating Agency Identifier
OTP	One-time Password
PBX	Private Branch Exchange
PCSC	Preventing and Combating Serious Crime
PDA	Personal Digital Assistant
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
POC	Point-of-Contact
PSTN	Public Switched Telephone Network
QA	Quality Assurance
QoS	Quality of Service
RCMP	Royal Canadian Mounted Police
RF	Radio Frequency
SA	Security Addendum
SCO	State Compact Officer
SIB	State Identification Bureau

SIG	Special Interest Group
SP	Special Publication
SPRC	Security Policy Resource Center
SSID	Service Set Identifier
TAC	Terminal Agency Coordinator
TLS	Transport Layer Security
UCN	Universal Control Number
VLAN	Virtual Local Area Network
VM	Virtual Machine
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

APPENDIX C NETWORK TOPOLOGY DIAGRAMS

Network diagrams, i.e. topological drawings, are an essential part of solid network security. Through graphical illustration, a comprehensive network diagram provides the “big picture” – enabling network managers to quickly ascertain the interconnecting nodes of a network for a multitude of purposes, including troubleshooting and optimization. Network diagrams are integral to demonstrating the manner in which each agency ensures criminal justice data is afforded appropriate technical security protections and is protected during transit and at rest.

The following diagrams, labeled Appendix C.1-A through C.1-D, are examples for agencies to utilize during the development, maintenance, and update stages of their own network diagrams. By using these example drawings as a guideline, agencies can form the foundation for ensuring compliance with Section 5.7.1.2 of the CJIS Security Policy.

The purpose for including the following diagrams in this Policy is to aid agencies in their understanding of diagram expectations and should not be construed as a mandated method for network topologies. It should also be noted that agencies are not required to use the identical icons depicted in the example diagrams and should not construe any depiction of a particular vendor product as an endorsement of that product by the FBI CJIS Division.

Appendix C.1-A is a conceptual overview of the various types of agencies that can be involved in handling of CJ, and illustrates several ways in which these interconnections might occur. This diagram is not intended to demonstrate the level of detail required for any given agency’s documentation, but it provides the reader with some additional context through which to digest the following diagrams. Take particular note of the types of network interfaces in use between agencies, in some cases dedicated circuits with encryption mechanisms, and in other cases VPNs over the Internet. This diagram attempts to show the level of diversity possible within the law enforcement community. These diagrams in no way constitute a standard for network engineering, but rather, for the expected quality of documentation.

The next three topology diagrams, C.1-B through C.1-D, depict conceptual agencies. For C.1-B through C.1-D, the details identifying specific “moving parts” in the diagrams by manufacturer and model are omitted, but it is expected that any agencies producing such documentation will provide diagrams with full manufacturer and model detail for each element of the diagram. Note that the quantities of clients should be documented in order to assist the auditor in understanding the scale of assets and information being protected.

Appendix C.1-B depicts a conceptual state law enforcement agency’s network topology and demonstrates a number of common technologies that are in use throughout the law enforcement community (some of which are compulsory per CJIS policy, and some of which are optional) including Mobile Broadband cards, VPNs, Firewalls, Intrusion Detection Devices, VLANs, and so forth. Note that although most state agencies will likely have highly-available configurations, the example diagram shown omits these complexities and only shows the “major moving parts” for clarity but please note the Policy requires the logical location of all components be shown. The level of detail depicted should provide the reader with a pattern to model future documentation from, but should not be taken as network engineering guidance.

Appendix C.1-C depicts a conceptual county law enforcement agency. A number of common technologies are presented merely to reflect the diversity in the community, including proprietary

Packet-over-RF infrastructures and advanced authentication techniques, and to demonstrate the fact that agencies can act as proxies for other agencies.

Appendix C.1-D depicts a conceptual municipal law enforcement agency, presumably a small one that lacks any precinct-to-patrol data communications. This represents one of the smallest designs that could be assembled that, assuming all other details are properly considered, would meet the criteria for Section 5.7.1.2. This diagram helps to demonstrate the diversity in size that agencies handling criminal justice data exhibit.

Figure C-1-A Overview: Conceptual Connections Between Various Agencies

Overview: Conceptual Connections Between Various Agencies

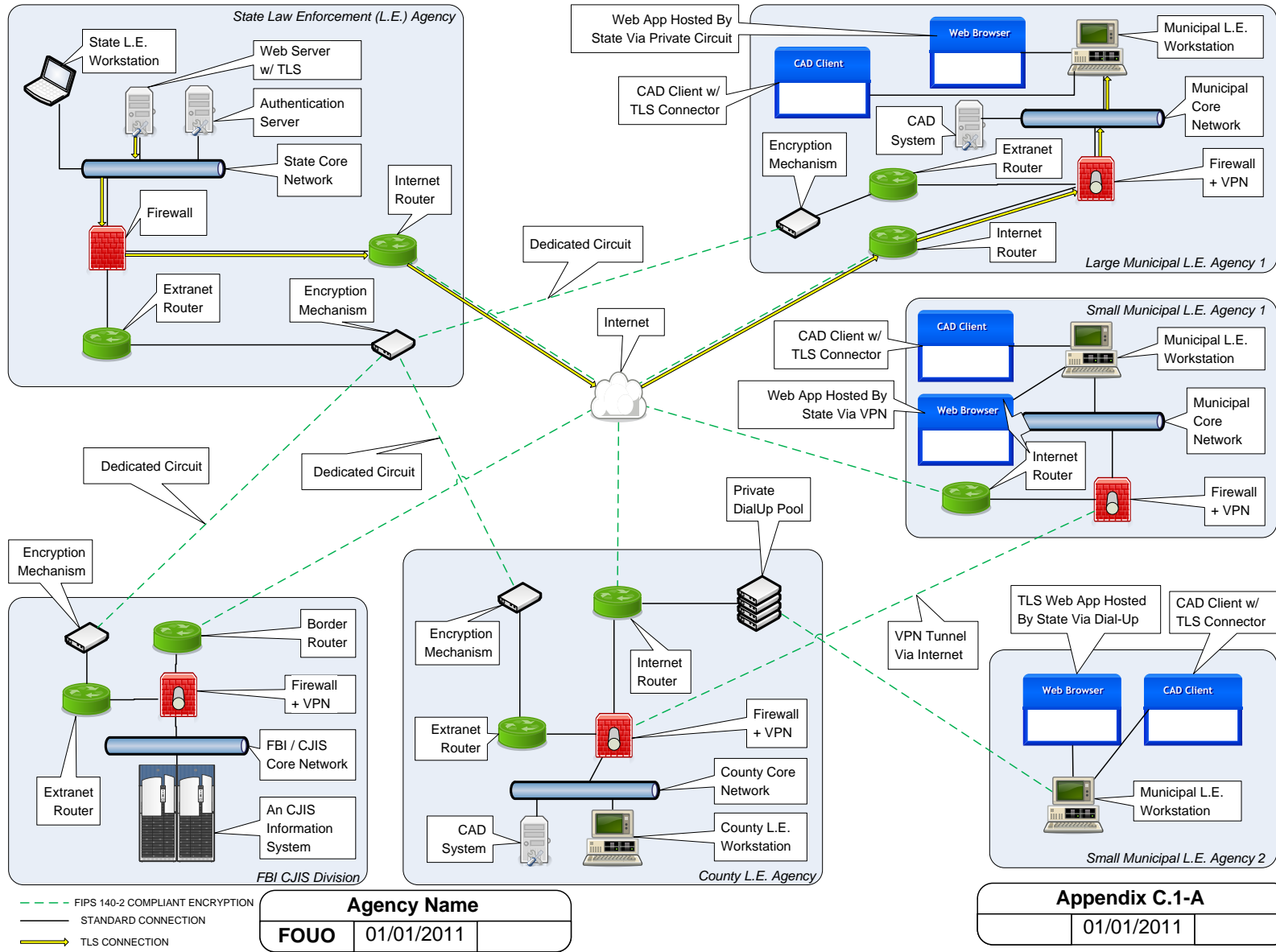
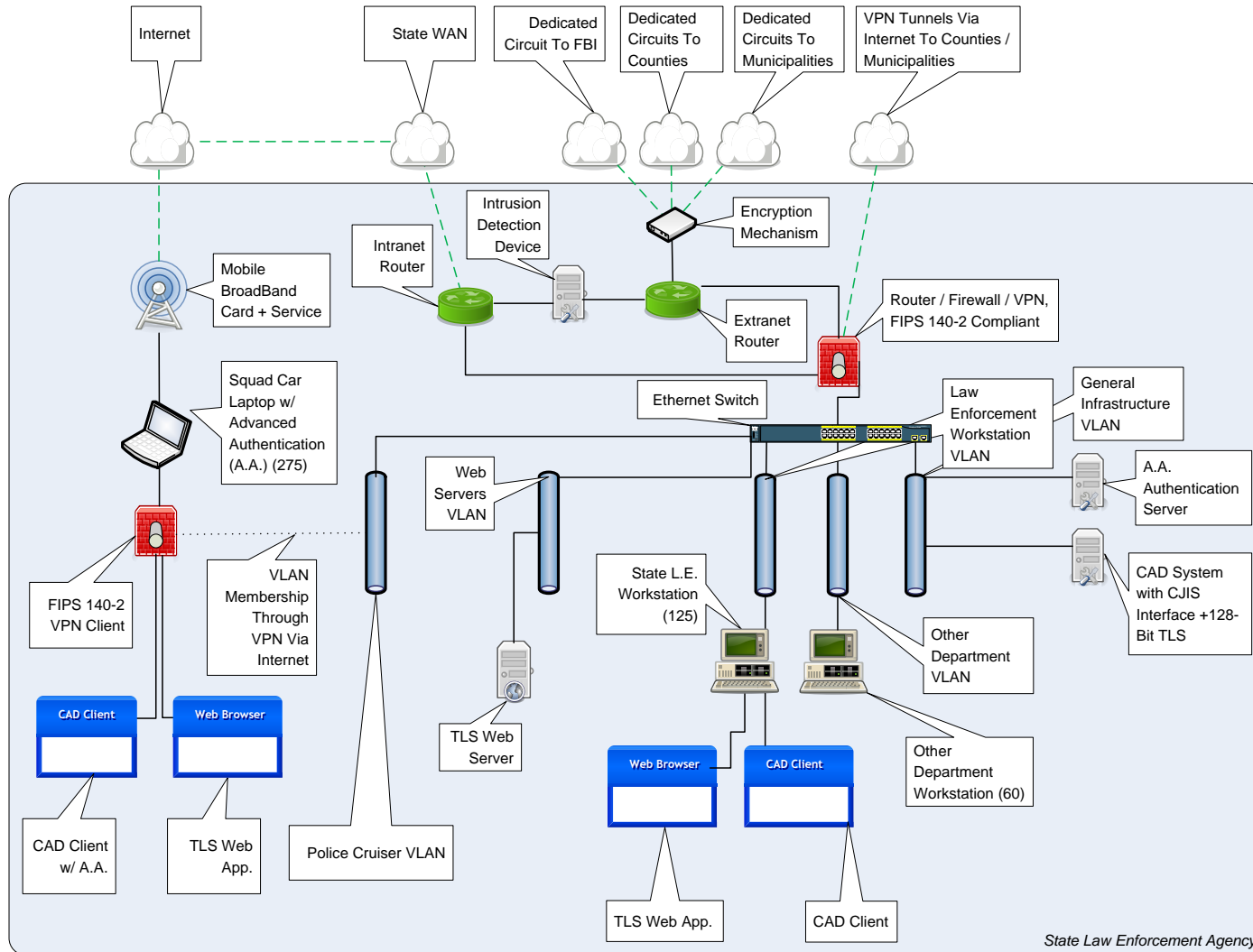


Figure C-1-B Conceptual Topology Diagram for a State Law Enforcement Agency

Conceptual Topology Diagram For A State Law Enforcement Agency



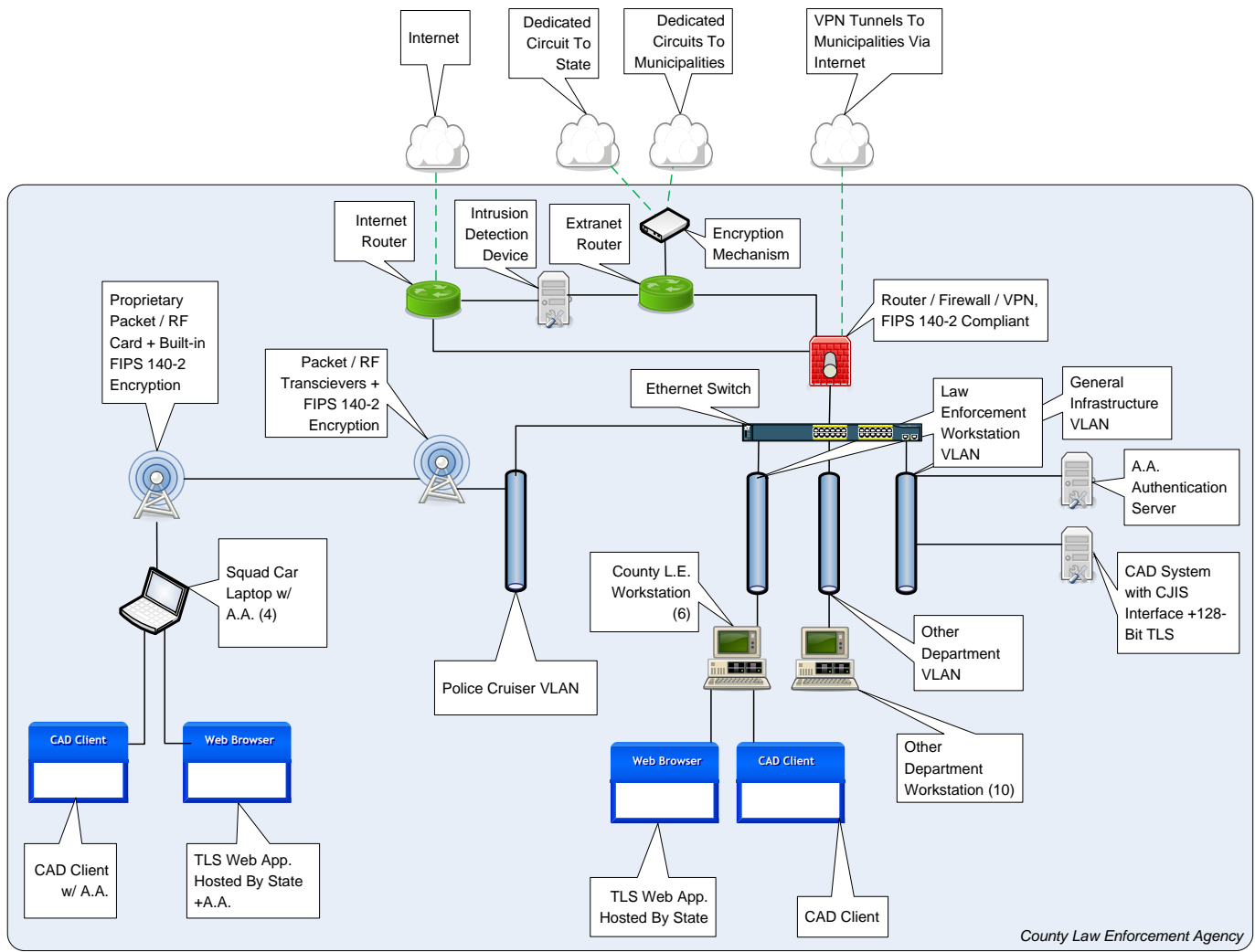
--- FIPS 140-2 COMPLIANT ENCRYPTION
 ——— STANDARD CONNECTION

Sample State Agency		
FOUO	01/01/2011	

Appendix C.1-B		
	01/01/2011	

Figure C-1-C Conceptual Topology Diagram for a County Law Enforcement Agency

Conceptual Topology Diagram For A County Law Enforcement Agency



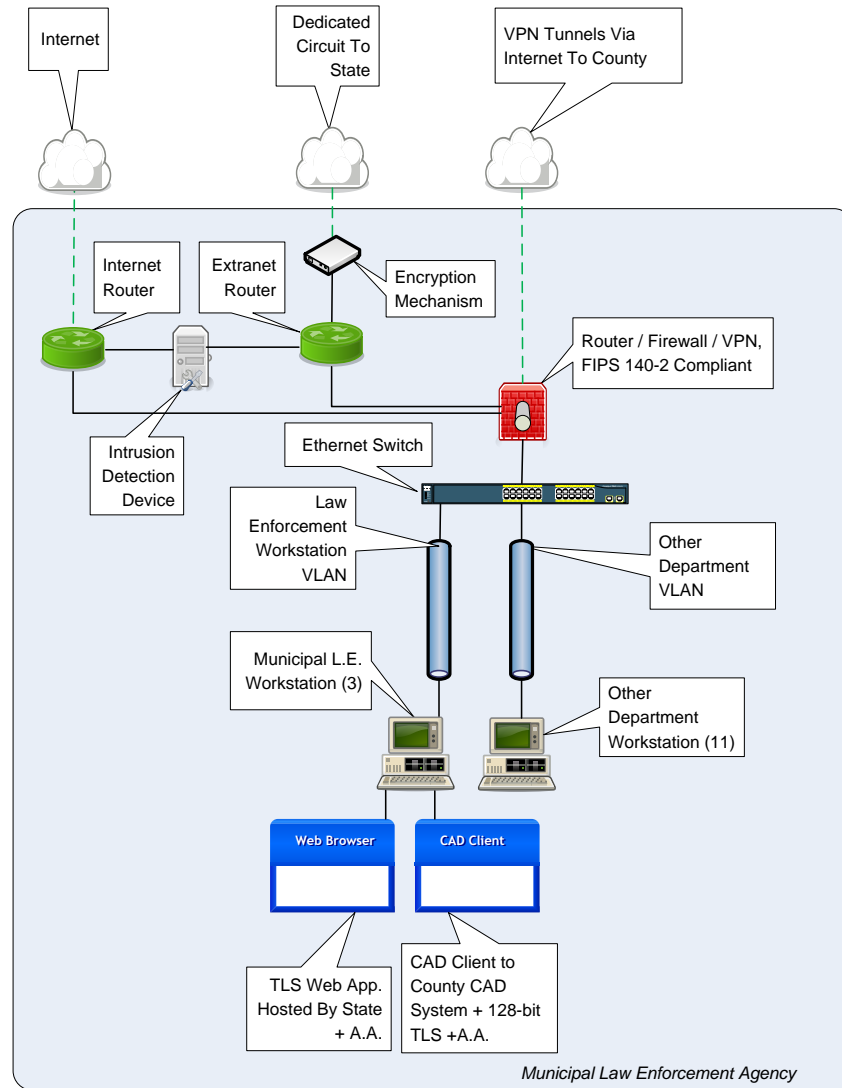
--- FIPS 140-2 COMPLIANT ENCRYPTION
 ——— STANDARD CONNECTION

Sample County Agency		
FOUO	01/01/2011	

Appendix C.1-C		
	01/01/2011	

Figure C-1-D Conceptual Topology Diagram for a Municipal Law Enforcement Agency

Conceptual Topology Diagram For A Municipal Law Enforcement Agency



--- FIPS 140-2 COMPLIANT ENCRYPTION
 ——— STANDARD CONNECTION

Sample Municipal Agency		
FOUO	01/01/2011	

Appendix C.1-D		
	01/01/2011	

APPENDIX D SAMPLE INFORMATION EXCHANGE AGREEMENTS

D.1 CJIS User Agreement

CRIMINAL JUSTICE INFORMATION SERVICES (CJIS) SYSTEMS USER AGREEMENT

The FBI CJIS Division provides state-of-the-art identification and information services to the local, state, tribal, federal, and international criminal justice communities, as well as the noncriminal justice community, for licensing and employment purposes. These services are administered and maintained by the FBI CJIS Division and managed in cooperation with the CJIS Systems Agency (CSA) and its administrator for CJIS data, the CJIS Systems Officer (CSO). The CJIS Systems include, but are not limited to: the Interstate Identification Index (III); National Crime Information Center (NCIC); Uniform Crime Reporting (UCR), whether summary or incident-based reporting to the National Incident-Based Reporting System; Fingerprint Identification Record System; Law Enforcement National Data Exchange (N-DEx); Law Enforcement Enterprise Portal; and the National Instant Criminal Background Check System (NICS).

The FBI CJIS Division provides the following services to its users, as applicable:

1. Operational, technical, and investigative assistance.
2. Telecommunication lines to state, federal, and regulatory interfaces.
3. Legal and legislative review of matters pertaining to all CJIS Systems.
4. Timely information on all aspects of all CJIS Systems and other related programs by means of operating manuals, code manuals, technical and operational updates, various newsletters, information letters, frequently asked questions, and other relevant documents.
5. Training assistance and up-to-date materials provided to each CSO, NICS Point of Contact (POC), state Compact Officer, State Administrator, Information Security Officer (ISO), and other appropriate personnel.
6. Ongoing assistance to Systems' users through meetings and briefings with the CSOs, State Administrators, Compact Officers, ISOs, and NICS State POCs to discuss operational and policy issues.
7. Advisory Process through which authorized users have input as to the policies and procedures governing the operation of CJIS programs.

8. National Crime Prevention and Privacy Compact Administrative Office through which states and other authorized users may submit issues concerning the noncriminal justice use of the III System.
9. Annual NICS Users Conference.
10. Audit.
11. Staff research assistance.

PART 1

The purpose behind a designated CSO is to unify responsibility for Systems user discipline and to ensure adherence to established procedures and policies within each signatory state/territory/tribal agency and by each federal user. This agreement outlines the responsibilities of each CSO as they relate to all CJIS Systems and other related CJIS administered programs. These individuals are ultimately responsible for planning necessary hardware, software, funding, and training for access to all CJIS Systems.

To ensure continued access as set forth above, the CSA agrees to adhere to all applicable CJIS policies including, but not limited to, the following:

1. The signatory state/tribal agency will provide fingerprints that meet submission criteria for all qualifying arrests. In addition, states/tribal agencies will make their records available for interstate exchange for criminal justice and other authorized purposes unless restricted by state/tribal law, and, where applicable, continue to move toward participation in the III and, upon ratification of the National Crime Prevention and Privacy Compact, the National Fingerprint File.
2. Appropriate and reasonable quality assurance procedures; e.g., hit confirmation, audits for record timeliness, and validation, must be in place to ensure that only complete, accurate, and valid information is maintained in the CJIS Systems.
3. Biannual file synchronization of information entered into the III by participating states.
4. Security - Each agency is responsible for appropriate security measures as applicable to physical security of terminals and telecommunication lines; personnel security to include background screening requirements; technical security to protect against unauthorized use; data security to include III use, dissemination, and logging; and security of criminal history

records. Additionally, each CSO must ensure that all agencies establish an information security structure that provides for an ISO and complies with the CJIS Security Policy.

5. Audit - Each agency shall be responsible for complying with all audit requirements for use of CJIS Systems. Each CSO is responsible for completing a triennial audit of all agencies with access to CJIS Systems through the CSO's lines.
6. Training - Each agency shall be responsible for training requirements, including compliance with operator training mandates.
7. Integrity of the Systems - Each agency shall be responsible for maintaining the integrity of the system in accordance with FBI CJIS Division/state/federal/tribal policies to ensure only authorized terminal access; only authorized transaction submission; and proper handling and dissemination of CJ. Each agency shall also be responsible for computer security incident reporting as required by the *CJIS Security Policy*.

The following documents are incorporated by reference and made part of this agreement for CSA users:

1. Bylaws for the CJIS Advisory Policy Board and Working Groups.
2. CJIS Security Policy.
3. Interstate Identification Index Operational and Technical Manual, National Fingerprint File Operations Plan, NCIC 2000 Operating Manual, UCR Handbook-NIBRS Edition, and National Incident-Based Reporting System Volumes 1, 2, and 4.
4. National Crime Prevention and Privacy Compact, 42 United States Code (U.S.C.) §14616.
5. NCIC Standards and UCR Standards, as recommended by the CJIS Advisory Policy Board.
6. The National Fingerprint File Qualification Requirements.
7. Title 28, Code of Federal Regulations, Parts 20 and 25, §50.12, and Chapter IX.
8. Electronic Fingerprint Transmission Specifications.

9. Other relevant documents, to include: NCIC Technical and Operational Updates, CJIS Information Letters, NICS User Manual, NICS Interface Control Document.
10. Applicable federal, state, and tribal laws and regulations.

PART 2

Additionally, there are authorized federal regulatory recipients and other authorized users that provide electronic fingerprint submissions through a CJIS Wide Area Network (WAN) connection (or other approved form of electronic connection) to the CJIS Division that are required to comply with the following CJIS policies:

1. The authorized user will provide fingerprints that meet submission criteria and apply appropriate and reasonable quality assurance procedures.
2. Security - Each agency is responsible for appropriate security measures as applicable to physical security of communication equipment; personnel security to include background screening requirements; technical security to protect against unauthorized use; and security of criminal history records.
3. Audit - Each authorized user shall be responsible for complying with all audit requirements for CJIS Systems. Additionally, each authorized user is subject to a triennial audit by the CJIS Division Audit staff.
4. Training - Each authorized user receiving criminal history record information shall be responsible for training requirements, including compliance with proper handling of criminal history records.

The following documents are incorporated by reference and made part of this agreement for non-CSA authorized users:

1. CJIS Security Policy.
2. National Crime Prevention and Privacy Compact, 42 U.S.C. §14616.
3. Title 28, Code of Federal Regulations, Parts 20 and 25, § 50.12, and Chapter IX.
4. Other relevant documents, to include CJIS Information Letters.

5. Applicable federal, state, and tribal laws and regulations.

GENERAL PROVISIONS

Funding:

Unless otherwise agreed in writing, each party shall bear its own costs in relation to this agreement. Expenditures will be subject to federal and state budgetary processes and availability of funds pursuant to applicable laws and regulations. The parties expressly acknowledge that this in no way implies that Congress will appropriate funds for such expenditures.

Termination:

1. All activities of the parties under this agreement will be carried out in accordance to the above-described provisions.
2. This agreement may be amended or terminated by the mutual written consent of the parties authorized representatives.
3. Either party may terminate this agreement upon 30-days written notification to the other party. Such notice will be the subject of immediate consultation by the parties to decide upon the appropriate course of action. In the event of such termination, the following rules apply:
 - a. The parties will continue participation, financial or otherwise, up to the effective date of termination.
 - b. Each party will pay the costs it incurs as a result of termination.
 - c. All information and rights therein received under the provisions of this agreement prior to the termination will be retained by the parties, subject to the provisions of this agreement.

ACKNOWLEDGMENT AND CERTIFICATION

As a CSO or CJIS WAN Official (or other CJIS authorized official), I hereby acknowledge the duties and responsibilities as set out in this agreement. I acknowledge that these duties and responsibilities have been developed and approved by CJIS Systems users to ensure the reliability, confidentiality, completeness, and accuracy of all information contained in, or obtained by means of, the CJIS Systems. I further acknowledge that failure to comply with these duties and responsibilities may result in the imposition of sanctions against the offending state/agency; other federal, tribal, state, and local criminal justice users; and approved noncriminal justice users with System access, whether direct or indirect. The Director of the FBI (or the National Crime Prevention and Privacy Compact Council), may approve sanctions to include the termination of CJIS services.

I hereby certify that I am familiar with all applicable documents that are made part of this agreement and to all applicable federal and state laws and regulations relevant to the receipt and dissemination of documents provided through the CJIS Systems.

This agreement is a formal expression of the purpose and intent of both parties and is effective when signed. It may be amended by the deletion or modification of any provision contained therein, or by the addition of new provisions, after written concurrence of both parties. The "Acknowledgment and Certification" is being executed by the CSO or CJIS WAN Official (or other CJIS authorized official) in both an individual and representative capacity. Accordingly, this agreement will remain in effect after the CSO or CJIS WAN Official (or other CJIS authorized official) vacates his/her position or until it is affirmatively amended or rescinded in writing. This agreement does not confer, grant, or authorize any rights, privileges, or obligations to any third party.

SYSTEMS USER AGREEMENT

Please execute either Part 1 or Part 2

PART 1

_____ Date: _____
CJIS Systems Officer

Printed Name/Title

CONCURRENCE OF CSA HEAD:
_____ Date: _____
CSA Head

Printed Name/Title

PART 2

_____ Date: _____
CJIS WAN Official (or other CJIS Authorized Official)

Printed Name/Title

CONCURRENCE OF CJIS WAN AGENCY HEAD:
_____ Date: _____
CJIS WAN Agency Head

Printed Name/Title

FBI CJIS DIVISION:

Date: _____

[Name]

Assistant Director

FBI CJIS Division

* The FBI Designated Federal Officer should be notified when a CSO or other CJIS WAN/authorized Official vacates his/her position. The name and telephone number of the Acting CSO or other CJIS WAN/authorized Official, and when known, the name and telephone number of the new CSO or other CJIS WAN/authorized Official, should be provided. Revised: 05/03/2006

D.2 Management Control Agreement

Management Control Agreement

Pursuant to the CJIS Security Policy, it is agreed that with respect to administration of that portion of computer systems and network infrastructure interfacing directly or indirectly with the state network (Network Name) for the interstate exchange of criminal history/criminal justice information, the (Criminal Justice Agency) shall have the authority, via managed control, to set, maintain, and enforce:

- (1) Priorities.
- (2) Standards for the selection, supervision, and termination of personnel access to Criminal Justice Information (CJI).
- (3) Policy governing operation of justice systems, computers, access devices, circuits, hubs, routers, firewalls, and any other components, including encryption, that comprise and support a telecommunications network and related criminal justice systems to include but not limited to criminal history record/criminal justice information, insofar as the equipment is used to process or transmit criminal justice systems information guaranteeing the priority, integrity, and availability of service needed by the criminal justice community.
- (4) Restriction of unauthorized personnel from access or use of equipment accessing the State network.
- (5) Compliance with all rules and regulations of the (Criminal Justice Agency) Policies and CJIS Security Policy in the operation of all information received.

“...management control of the criminal justice function remains solely with the Criminal Justice Agency.” Section 5.1.1.4

This agreement covers the overall supervision of all (Criminal Justice Agency) systems, applications, equipment, systems design, programming, and operational procedures associated with the development, implementation, and maintenance of any (Criminal Justice Agency) system to include NCIC Programs that may be subsequently designed and/or implemented within the (Criminal Justice Agency).

John Smith, CIO
Any State Department of Administration

Date

Joan Brown, CIO
(Criminal Justice Agency)

Date

D.3 Noncriminal Justice Agency Agreement & Memorandum of Understanding

MEMORANDUM OF UNDERSTANDING

BETWEEN

THE FEDERAL BUREAU OF INVESTIGATION

AND

(Insert Name of Requesting Organization)

FOR

THE ESTABLISHMENT AND ACCOMMODATION OF
THIRD-PARTY CONNECTIVITY TO THE
CRIMINAL JUSTICE INFORMATION SERVICES DIVISION'S WIDE AREA NETWORK

1. **PURPOSE:** This Memorandum of Understanding (MOU) between the Federal Bureau of Investigation (FBI) and **(insert requesting organization's name)**, hereinafter referred to as the "parties," memorializes each party's responsibilities with regard to establishing connectivity to records services accessible via the Wide Area Network (WAN) of the FBI's Criminal Justice Information Services (CJIS) Division.
2. **BACKGROUND:** The requesting organization, **(insert requesting organization's name)**, being approved for access to systems of records accessible via the CJIS WAN, desires connectivity to the CJIS WAN or via a secure Virtual Private Network (VPN) Connection (Internet) to the CJIS WAN. The CJIS Division has created a framework for accommodating such requests based on the type of connection.

In preparing for such non-CJIS-funded connectivity to the CJIS WAN, the parties plan to acquire, configure, and place needed communications equipment at suitable sites and to make electronic connections to the appropriate systems of records via the CJIS WAN.

To ensure that there is a clear understanding between the parties regarding their respective roles in this process, this MOU memorializes each party's responsibilities regarding the development, operation, and maintenance of third-party connectivity to the CJIS WAN. Unless otherwise contained in an associated contract, the enclosed terms apply. If there is a conflict between terms and provisions contained in both the contract and this MOU, the contract will prevail.

3. **AUTHORITY:** The FBI is entering into this MOU under the authority provided by Title 28, United States Code (U.S.C.), Section 534; 42 U.S.C. § 14616; and/or Title 28, Code of Federal Regulations, Part 906.

4. **SCOPE:**

a. The CJIS Division agrees to:

i. Provide the requesting organization with a "CJIS WAN Third-Party Connectivity Package" that will detail connectivity requirements and options compatible with the CJIS Division's WAN architecture upon receipt of a signed nondisclosure statement.

ii. Configure the requesting organization's connection termination equipment suite at Clarksburg, West Virginia, and prepare it for deployment or shipment under the CJIS WAN option. In the Secure VPN arrangement only, the third party will develop, configure, manage, and maintain its network connectivity to its preferred service provider.

iii. Work with the requesting organization to install the connection termination equipment suite and verify connectivity.

iv. Perform installation and/or routine maintenance on the requesting organization's third-party dedicated CJIS WAN connection termination equipment after coordinating with the requesting organization's designated point of contact (POC) and during a time when the CJIS Division's technical personnel are near the requesting organization's site.

v. Perform periodic monitoring and troubleshooting of the requesting organization's CJIS WAN connection termination equipment. Software patches will be maintained on the dedicated CJIS WAN connected network equipment only. Under the Secure VPN option, no availability or data thru-put rates will be guaranteed.

vi. Provide 24 hours a day, 7 days a week uninterrupted monitoring from the CJIS Division's Network Operations Center.

vii. Provide information regarding potential hardware end-of-life replacement cycles to the requesting organization for its budgeting purposes.

viii. Maintain third-party dedicated CJIS WAN connection termination equipment as if in the CJIS Division's operational environment.

ix. Update the appropriate software on the requesting organization's dedicated connection termination equipment connected to the CJIS WAN (i.e., Cisco Internetwork Operating System, SafeNet frame relay encryptor firmware, etc.) pursuant to the requesting organization's authorized maintenance contracts.

x. Provide a POC and telephone number for MOU-related issues.

b. The **(insert requesting organization's name)** agrees to:

i. Coordinate requests for third-party connectivity to the CJIS WAN or the Secure VPN with the CJIS Division's POC.

ii. Purchase hardware and software that are compatible with the CJIS WAN.

iii. Pay for the telecommunications infrastructure that supports its connection to the CJIS WAN or Secure VPN.

iv. Maintain telecommunication infrastructure in support of Secure VPN connectivity.

v. Provide any/all hardware and software replacements and upgrades as mutually agreed to by the parties.

vi. Pay for all telecommunication requirements related to its connectivity.

vii. Provide required information for dedicated service relating to Data Link Connection Identifiers, Circuit Identifier, Permanent Virtual Circuit Identifiers, Local Exchange Carrier Identifier, POC, location, etc., as determined by the parties.

viii. Transport the CJIS WAN connection termination equipment suite to the CJIS Division for configuration and preparation for deployment under the dedicated service option.

ix. Provide registered Internet Protocol information to be used by the requesting organization's system to the CJIS Division.

x. Provide the CJIS Division with six months advance notice or stated amount of time for testing activities (i.e., disaster recovery exercises).

xi. Provide the CJIS Division with applicable equipment maintenance contract numbers and level of service verifications needed to perform software upgrades on connection termination equipment.

xii. Provide the CJIS Division with applicable software upgrade and patch images (or information allowing the CJIS Division to access such images).

xiii. Transport only official, authorized traffic over the Secure VPN.

xiv. Provide a POC and telephone number for MOU-related issues.

5. **FUNDING:** There are no reimbursable expenses associated with this level of support. Each party will fund its own activities unless otherwise agreed to in writing. This MOU is not an obligation or commitment of funds, nor a basis for transfer of funds, but rather is a basic statement of understanding between the parties hereto of the nature of the relationship for the connectivity efforts. Unless otherwise agreed to in writing, each party shall bear its own costs in relation to this MOU. Expenditures by each party will be subject to its budgetary processes and to the availability of funds and resources pursuant to applicable laws, regulations, and policies. The parties expressly acknowledge that the above language in no way implies that Congress will appropriate funds for such expenditures.

6. **SETTLEMENT OF DISPUTES:** Disagreements between the parties arising under or relating to this MOU will be resolved only by consultation between the parties and will not be referred to any other person or entity for settlement.

7. SECURITY: It is the intent of the parties that the actions carried out under this MOU will be conducted at the unclassified level. No classified information will be provided or generated under this MOU.

8. AMENDMENT, TERMINATION, ENTRY INTO FORCE, AND DURATION:

a. All activities of the parties under this MOU will be carried out in accordance with the above - described provisions.

b. This MOU may be amended or terminated by the mutual written consent of the parties' authorized representatives.

c. Either party may terminate this MOU upon 30-days written notification to the other party. Such notice will be the subject of immediate consultation by the parties to decide upon the appropriate course of action. In the event of such termination, the following rules apply:

i. The parties will continue participation, financial or otherwise, up to the effective date of the termination.

ii. Each party will pay the costs it incurs as a result of the termination.

iii. All information and rights therein received under the provisions of this MOU prior to the termination will be retained by the parties, subject to the provisions of this MOU.

9. FORCE AND EFFECT: This MOU, which consists of nine numbered sections, will enter into effect upon signature of the parties and will remain in effect until terminated. The parties should review the contents of this MOU annually to determine whether there is a need for the deletion, addition, or amendment of any provision. This MOU is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law or otherwise by any third party against the parties, their parent agencies, the United States, or the officers, employees, agents, or other associated personnel thereof.

The foregoing represents the understandings reached between the parties.

FOR THE FEDERAL BUREAU OF INVESTIGATION

[Name]

Date

Assistant Director

Criminal Justice Information Services Division

FOR THE (insert requesting organization name)

Date

D.4 Interagency Connection Agreement

CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)

Wide Area Network (WAN) USER AGREEMENT

BY INTERIM REMOTE LATENT USERS

The responsibility of the FBI CJIS Division is to provide state-of-the-art identification and information services to the local, state, federal, and international criminal justice communities, as well as the civil community for licensing and employment purposes. The data provided by the information systems administered and maintained by the FBI CJIS Division are routed to and managed in cooperation with the designated interface agency official. This information includes, but is not limited to, the Interstate Identification Index (III), National Crime Information Center (NCIC), Uniform Crime Reporting (UCR)/National Incident-Based Reporting System (NIBRS), and the Integrated Automated Fingerprint Identification System (IAFIS) programs.

In order to fulfill this responsibility, the FBI CJIS Division provides the following services to its users:

- Operational, technical, and investigative assistance;
- Telecommunications lines to local, state, federal and authorized interfaces;
- Legal and legislative review of matters pertaining to IAFIS, CJIS WAN and other related services;
- Timely information on all aspects of IAFIS, CJIS WAN, and other related programs by means of technical and operational updates, various newsletters, and other relative documents;
- Shared management through the CJIS Advisory Process and the Compact Council;
- Training assistance and up-to-date materials provided to each designated agency official, and;
- Audit.

The concept behind a designated interface agency official is to unify responsibility for system user discipline and ensure adherence to system procedures and policies within each interface agency. These individuals are ultimately responsible for planning necessary hardware, software, funding, training, and the administration of policy and procedures including security and integrity for complete access to CJIS related systems and CJIS WAN related data services by authorized agencies.

The following documents and procedures are incorporated by reference and made part of this agreement:

- *CJIS Security Policy*;
- *Title 28, Code of Federal Regulations, Part 20*;
- Computer Incident Response Capability (CIRC);
- Applicable federal and state laws and regulations.

To ensure continued access as set forth above, the designated interface agency agrees to adhere to all CJIS policies, including, but not limited to, the following:

1. The signatory criminal agency will provide fingerprints for all qualifying arrests either via electronic submission or fingerprint card that meet submission criteria. In addition, the agency will make their records available for interstate exchange for criminal justice and other authorized purposes.
2. The signatory civil agency with legislative authority will provide all qualifying fingerprints via electronic submission or fingerprint card that meet submission criteria.
3. Appropriate and reasonable quality assurance procedures must be in place to ensure that only complete, accurate, and valid information is maintained in the system.
4. Security - Each agency is responsible for appropriate security measures as applicable to physical security of terminals and telecommunications lines; Interim Distributed Imaging System (IDIS) equipment shall remain stand-alone

devices and be used only for authorized purposes; personnel security to meet background screening requirements; technical security to protect against unauthorized use; data security, dissemination, and logging for audit purposes; and actual security of criminal history records. Additionally, each agency must establish an information security structure that provides for an Information Security Officer (ISO) or a security point of contact.

5. Audit - Each agency shall be responsible for complying with the appropriate audit requirements.
6. Training - Each agency shall be responsible for training requirements, including compliance with training mandates.
7. Integrity of the system shall be in accordance with FBI CJIS Division and interface agency policies. Computer incident reporting shall be implemented.

Until states are able to provide remote latent connectivity to their respective latent communities via a state WAN connection, the CJIS Division may provide direct connectivity to IAFIS via a dial-up connection or through the Combined DNA Index System (CODIS) and/or National Integrated Ballistics Information Network (NIBIN) connections. When a state implements a latent management system and is able to provide intrastate connectivity and subsequent forwarding to IAFIS, this agreement may be terminated. Such termination notice will be provided in writing by either the FBI or the state CJIS Systems Agency.

It is the responsibility of the local remote latent user to develop or acquire an IAFIS compatible workstation. These workstations may use the software provided by the FBI or develop their own software, provided it is IAFIS compliant.

The CJIS Division will provide the approved modem and encryptors required for each dial-up connection to IAFIS. The CJIS Communication Technologies Unit will configure and test the encryptors before they are provided to the user. Users requesting remote latent connectivity through an existing CODIS and/or NIBIN connection must receive verification from the FBI that there are a sufficient number of Ethernet ports on the router to accommodate the request.

If at any time search limits are imposed by the CJIS Division, these individual agency connections will be counted toward the total state allotment.

FBI CJIS DIVISION:

Signature – [Name]

Assistant Director _____
Title Date

* If there is a change in the CJIS WAN interface agency official, the FBI Designated Federal Employee must be notified in writing 30 days prior to the change.

5/27/2004 UA modification reflects change in CTO title to CSO.

APPENDIX E SECURITY FORUMS AND ORGANIZATIONAL ENTITIES

Online Security Forums / Organizational Entities
AntiOnline
Black Hat
CIO.com
CSO Online
CyberSpeak Podcast
FBI Criminal Justice Information Services Division (CJIS)
Forrester Security Forum
Forum of Incident Response and Security Teams (FIRST)
Information Security Forum (ISF)
Information Systems Audit and Control Association (ISACA)
Information Systems Security Association (ISSA)
Infosyssec
International Organization for Standardization (ISO)
International Information Systems Security Certification Consortium, Inc. (ISC) ²
Metasploit
Microsoft Developer Network (MSDN) Information Security
National Institute of Standards and Technology (NIST)
Open Web Application Security Project (OWASP)
SANS (SysAdmin, Audit, Network, Security) Institute
SC Magazine
Schneier.com
Security Focus
The Register
US Computer Emergency Response Team (CERT)
US DoJ Computer Crime and Intellectual Property Section (CCIPS)

APPENDIX F SAMPLE FORMS

This appendix contains sample forms.

F.1 Security Incident Response Form

**FBI CJIS DIVISION
INFORMATION SECURITY OFFICER (ISO)
SECURITY INCIDENT REPORTING FORM**

NAME OF PERSON REPORTING THE INCIDENT: _____

DATE OF REPORT: _____ (mm/dd/yyyy)

DATE OF INCIDENT: _____ (mm/dd/yyyy)

POINT(S) OF CONTACT (Include Phone/Extension/Email): _____

LOCATION(S) OF INCIDENT: _____

INCIDENT DESCRIPTION: _____

SYSTEM(S) AFFECTED: _____

SYSTEM(S) AFFECTED (e.g. CAD, RMS, file server, etc.): _____

METHOD OF DETECTION: _____

ACTIONS TAKEN/RESOLUTION: _____

Copies To:

John C. Weatherly

(FBI CJIS Division ISO)

1000 Custer Hollow Road

Clarksburg, WV 26306-0102

(304) 625-3660

iso@fbi.gov

APPENDIX G BEST PRACTICES

G.1 Virtualization

Virtualization

This appendix documents security considerations for implementing and operating virtual environments that process, store, and/or transmit Criminal Justice Information.

The FBI CJIS ISO has fielded several inquiries from various states requesting guidance on implementing virtual environments within their data centers. With the proliferation of virtual environments across industry in general there is a realistic expectation that FBI CJIS Auditors will encounter virtual environments during the upcoming year. Criminal Justice Agencies (CJAs) and Noncriminal Justice Agencies (NCJAs) alike need to understand and appreciate the foundation of security protection measures required for virtual environments.

From Microsoft's Introduction to Windows Server 2008

<http://www.microsoft.com/windowsserver2008/en/us/hyperv.aspx>:

“Server virtualization, also known as hardware virtualization, is a hot topic in the IT world because of the potential for serious economic benefits. Server virtualization enables multiple operating systems to run on a single physical machine as virtual machines (VMs). With server virtualization, you can consolidate workloads across multiple underutilized server machines onto a smaller number of machines. Fewer physical machines can lead to reduced costs through lower hardware, energy, and management overhead, plus the creation of a more dynamic IT infrastructure.”

From a trade publication, kernelthread.com

<http://www.kernelthread.com/publications/virtualization/>:

“Virtualization is a framework or methodology of dividing the resources of a computer into multiple execution environments, by applying one or more concepts or technologies such as hardware and software partitioning, time-sharing, partial or complete machine simulation, emulation, quality of service, and many others.”

From an Open Source Software developer

<http://www.kallasoft.com/pc-hardware-virtualization-basics/>:

“Virtualization refers to virtualizing hardware in software, allowing multiple operating systems, or images, to run concurrently on the same hardware. There are two main types of virtualization software:

- *“Type-1 Hypervisor, which runs ‘bare-metal’ (on top of the hardware)*
- *“Type-2 Hypervisor which requires a separate application to run within an operating system*

“Type1 hypervisors usually offer the best in efficiency, while Type-2 hypervisors allow for greater support of hardware that can be provided by the operating system. For the developer, power user, and small business IT professionals, virtualization offers the same basic idea of collapsing multiple physical boxes into one. For instance, a small business can run a web server and an Exchange server without the need for two boxes. Developers and power users can use the ability to contain different development environments without the need to modify their main operating system. Big businesses can also benefit from virtualization by allowing software maintenance to be run and tested on a separate image on hardware without having to take down the main production system.”

Industry leaders and niche developers are bringing more products to market every day. The following article excerpts, all posted during September 2008, on www.virtualization.com are examples of industry offerings.

“Microsoft and Novell partnered together for joint virtualization solution. Microsoft and Novell are announcing the availability of a joint virtualization solution optimized for customers running mixed-source environments. The joint offering includes SUSE Linux Enterprise Server configured and tested as an optimized guest operating system running on Windows Server 2008 Hyper-V, and is fully supported by both companies’ channel partners. The offering provides customers with the first complete, fully supported and optimized virtualization solution to span Windows and Linux environments.”

“Sun Microsystems today announce the availability of Sun xVM Server software and Sun xVM Ops Center 2.0, key components in its strategy. Sun also announced the addition of comprehensive services and support for Sun xVM Server software and xVM Ops Center 2.0 to its virtualization suite of services. Additionally, Sun launched xVMserver.org, a new open source community, where developers can download the first source code bundle for Sun xVM Server software and contribute to the direction and development of the product.”

“NetEx, specialist in high-speed data transport over TCP, today announced Virtual HyperIP bandwidth optimization solutions for VMware environments that deliver a threefold to tenfold increase in data replication performance. Virtual HyperIP is a software-based Data Transport Optimizer that operates on the VMware ESX server and boosts the performance of storage replication applications from vendors such as EMC, NetApp, Symantec, IBM, Data Domain, and FalconStor. Virtual HyperIP mitigates TCP performance issues that are common when moving data over wide-area network (WAN) connections because of bandwidth restrictions, latency due to distance and/or router hop counts, packet loss and network errors. Like the company’s award-winning appliance-based HyperIP, Virtual HyperIP eliminates these issues with an innovative software design developed specifically to accelerate traffic over an IP based network.”

From several sources, particularly:

<http://www.windowsecurity.com/articles/security-virtualization.html>

<http://csrc.nist.gov/publications/drafts/6--64rev2/draft-sp800-64-Revision2.pdf>

Virtualization provides several benefits:

- Make better use of under-utilized servers by consolidating to fewer machines saving on hardware, environmental costs, management, and administration of the server infrastructure.
- Legacy applications unable to run on newer hardware and/or operating systems can be loaded into a virtual environment – replicating the legacy environment.
- Provides for isolated portions of a server where trusted and untrusted applications can be ran simultaneously – enabling hot standbys for failover.
- Enables existing operating systems to run on shared memory multiprocessors.
- System migration, backup, and recovery are easier and more manageable.

Virtualization also introduces several vulnerabilities:

- Host Dependent.
- If the host machine has a problem then all the VMs could potentially terminate.
- Compromise of the host makes it possible to take down the client servers hosted on the primary host machine.
- If the virtual network is compromised then the client is also compromised.
- Client share and host share can be exploited on both instances. Potentially this can lead to files being copied to the share that fill up the drive.

These vulnerabilities can be mitigated by the following factors:

- Apply “least privilege” technique to reduce the attack surface area of the virtual environment and access to the physical environment.
- Configuration and patch management of the virtual machine and host, i.e. Keep operating systems and application patches up to date on both virtual machines and hosts.
- Install the minimum applications needed on host machines.
- Practice isolation from host and virtual machine.
- Install and keep updated antivirus on virtual machines and the host.
- Segregation of administrative duties for host and versions.
- Audit logging as well as exporting and storing the logs outside the virtual environment.
- Encrypting network traffic between the virtual machine and host IDS and IPS monitoring.
- Firewall each virtual machine from each other and ensure that only allowed protocols will transact.

G.2 Voice over Internet Protocol

Voice over Internet Protocol (VoIP)

Attribution:

The following information has been extracted from NIST Special Publication 800-58, Security Considerations for Voice over IP Systems.

Definitions:

Voice over Internet Protocol (VoIP) – A set of software, hardware, and standards designed to make it possible to transmit voice over packet switched networks, either an internal Local Area Network, or across the Internet.

Internet Protocol (IP) - A protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP. IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses.

Summary:

Voice over Internet Protocol (VoIP) has been embraced by organizations globally as an addition to, or replacement for, public switched telephone network (PSTN) and private branch exchange (PBX) telephone systems. The immediate benefits are alluring since the typical cost to operate VoIP is less than traditional telephone services and VoIP can be installed in-line with an organization's existing Internet Protocol services. Unfortunately, installing a VoIP network is not a simple "plug-and-play" procedure. There are myriad security concerns, cost issues with new networking hardware requirements, and overarching quality of service (QoS) factors that have to be considered carefully.

What are some of the advantages of VoIP?

- a. Cost – a VoIP system is usually cheaper to operate than an equivalent office telephone system with a Private Branch Exchange and conventional telephone service.
- b. Integration with other services – innovative services are emerging that allow customers to combine web access with telephone features through a single PC or terminal. For example, a sales representative could discuss products with a customer using the company's web site. In addition, the VoIP system may be integrated with video across the Internet, providing a teleconferencing facility.

What are some of the disadvantages of VoIP?

- a. Startup cost – although VoIP can be expected to save money in the long run, the initial installation can be complex and expensive. In addition, a single standard has not yet emerged for many aspects of VoIP, so an organization must plan to support more than one standard, or expect to make relatively frequent changes as the VoIP field develops.
- b. Security – the flexibility of VoIP comes at a price: added complexity in securing voice and data. Because VoIP systems are connected to the data network, and share many of the same hardware and software components, there are more ways for intruders to attack a VoIP system than a conventional voice telephone system or PBX.

VoIP Risks, Threats, and Vulnerabilities

This section details some of the potential threats and vulnerabilities in a VoIP environment, including vulnerabilities of both VoIP phones and switches. Threat discussion is included because the varieties of threats faced by an organization determine the priorities in securing its communications equipment. Not all threats are present in all organizations. A commercial firm may be concerned primarily with toll fraud, while a government agency may need to prevent disclosure of sensitive information because of privacy or national security concerns. Information security risks can be broadly categorized into the following three types: confidentiality, integrity, and availability, (which can be remembered with the mnemonic “CIA”). Additional risks relevant to switches are fraud and risk of physical damage to the switch, physical network, or telephone extensions.

Packet networks depend for their successful operation on a large number of configurable parameters: IP and MAC (physical) addresses of voice terminals, addresses of routers and firewalls, and VoIP specific software such as Call Managers and other programs used to place and route calls. Many of these network parameters are established dynamically every time a network component is restarted, or when a VoIP telephone is restarted or added to the network. Because there are so many places in a network with dynamically configurable parameters, intruders have a wide array of potentially vulnerable points to attack.

Vulnerabilities described in this section are generic and may not apply to all systems, but investigations by NIST and other organizations have found these vulnerabilities in a number of VoIP systems. In addition, this list is not exhaustive; systems may have security weaknesses that are not included in the list. For each potential vulnerability, a recommendation is included to eliminate or reduce the risk of compromise.

Confidentiality and Privacy

Confidentiality refers to the need to keep information secure and private. For home computer users, this category includes confidential memoranda, financial information, and security information such as passwords. In a telecommunications switch, eavesdropping on conversations is an obvious concern, but the confidentiality of other information on the switch must be protected to defend against toll fraud, voice and data interception, and denial of service attacks. Network IP addresses, operating system type, telephone extension to IP address mappings, and communication protocols are all examples of information that, while not critical as individual pieces of data, can make an attacker’s job easier.

With conventional telephones, eavesdropping usually requires either physical access to tap a line, or penetration of a switch. Attempting physical access increases the intruder's risk of being discovered, and conventional PBXs have fewer points of access than VoIP systems. With VoIP, opportunities for eavesdroppers increase dramatically, because of the many nodes in a packet network.

Switch Default Password Vulnerability

It is common for switches to have a default login/password set, e.g., admin/admin, or root/root. This vulnerability also allows for wiretapping conversations on the network with port mirroring or bridging. An attacker with access to the switch administrative interface can mirror all packets on one port to another, allowing the indirect and unnoticeable interception of all communications. Failing to change default passwords is one of the most common errors made by inexperienced users.

REMEDIATION: If possible, remote access to the graphical user interface should be disabled to prevent the interception of plaintext administration sessions. Some devices provide the option of a direct USB connection in addition to remote access through a web browser interface. Disabling port mirroring on the switch should also be considered.

Classical Wiretap Vulnerability

Attaching a packet capture tool or protocol analyzer to the VoIP network segment makes it easy to intercept voice traffic.

REMEDIATION: A good physical security policy for the deployment environment is a general first step to maintaining confidentiality. Disabling the hubs on IP Phones as well as developing an alarm system for notifying the administrator when an IP Phone has been disconnected will allow for the possible detection of this kind of attack.

ARP Cache Poisoning and ARP Floods

Because many systems have little authentication, an intruder may be able to log onto a computer on the VoIP network segment, and then send ARP commands corrupting ARP caches on sender(s) of desired traffic, then activate IP. An ARP flood attack on the switch could render the network vulnerable to conversation eavesdropping. Broadcasting ARP replies blind is sufficient to corrupt many ARP caches. Corrupting the ARP cache makes it possible to re-route traffic to intercept voice and data traffic.

REMEDIATION: Use authentication mechanisms wherever possible and limit physical access to the VoIP network segment.

Web Server interfaces

Both VoIP switches and voice terminals are likely to have a web server interface for remote or local administration. An attacker may be able to sniff plaintext HTTP packets to gain confidential information. This would require access to the local network on which the server resides.

REMEDICATION: If possible, do not use an HTTP server. If it is necessary to use a web server for remote administration, use the more secure HTTPS (HTTP over SSL or TLS) protocol.

IP Phone Netmask Vulnerability

A similar effect of the ARP Cache Vulnerability can be achieved by assigning a subnet mask and router address to the phone crafted to cause most or all of the packets it transmits to be sent to an attacker's MAC address. Again, standard IP forwarding makes the intrusion all but undetectable.

REMEDICATION: A firewall filtering mechanism can reduce the probability of this attack. Remote access to IP phones is a severe risk.

Extension to IP Address Mapping Vulnerability

Discovering the IP address corresponding to any extension requires only calling that extension and getting an answer. A protocol analyzer or packet capture tool attached to the hub on the dialing instrument will see packets directly from the target instrument once the call is answered. Knowing the IP address of a particular extension is not a compromise in itself, but makes it easier to accomplish other attacks. For example, if the attacker is able to sniff packets on the local network used by the switch, it will be easy to pick out packets sent and received by a target phone. Without knowledge of the IP address of the target phone, the attacker's job may be much more difficult to accomplish and require much longer, possibly resulting in the attack being discovered.

REMEDICATION: Disabling the hub on the IP Phone will prevent this kind of attack. However, it is a rather simple task to turn the hub back on.

Integrity Issues

Integrity of information means that information remains unaltered by unauthorized users. For example, most users want to ensure that bank account numbers cannot be changed by anyone else, or that passwords are changed only by the user or an authorized security administrator. Telecommunication switches must protect the integrity of their system data and configuration. Because of the richness of feature sets available on switches, an attacker who can compromise the system configuration can accomplish nearly any other goal. For example, an ordinary extension could be re-assigned into a pool of phones that supervisors can listen in on or record conversations for quality control purposes. Damaging or deleting information about the IP network used by a VoIP switch results in an immediate denial of service.

The security system itself provides the capabilities for system abuse and misuse. That is, compromise of the security system not only allows system abuse but also allows the elimination of all traceability and the insertion of trapdoors for intruders to use on their next visit. For this reason, the security system must be carefully protected. Integrity threats include any in which system functions or data may be corrupted, either accidentally or as a result of malicious actions. Misuse may involve legitimate users (i.e. insiders performing unauthorized operations) or intruders.

A legitimate user may perform an incorrect, or unauthorized, operations function (e.g., by mistake or out of malice) and may cause deleterious modification, destruction, deletion, or disclosure of switch software and data. This threat may be caused by several factors including the possibility that the level of access permission granted to the user is higher than what the user needs to remain functional.

Intrusion - An intruder may masquerade as a legitimate user and access an operations port of the switch. There are a number of serious intrusion threats. For example, the intruder may use the permission level of the legitimate user and perform damaging operations functions such as:

- Disclosing confidential data
- Causing service deterioration by modifying the switch software
- Crashing the switch
- Removing all traces of the intrusion (e.g., modifying the security log) so that it may not be readily detected

Insecure state - At certain times the switch may be vulnerable due to the fact that it is not in a secure state. For example:

- After a system restart, the old security features may have been reset to insecure settings, and new features may not yet be activated. (For example, all old passwords may have reverted to the default system-password, even though new passwords are not yet assigned.) The same may happen at the time of a disaster recovery.
- At the time of installation the switch may be vulnerable until the default security features have been replaced.

DHCP Server Insertion Attack

It is often possible to change the configuration of a target phone by exploiting the DHCP response race when the IP phone boots. As soon as the IP phone requests a DHCP response, a rogue DHCP server can initiate a response with data fields containing false information.

This attack allows for possible man in the middle attacks on the IP-media gateway, and IP Phones. Many methods exist with the potential to reboot the phone remotely, e.g. “social engineering”, ping flood, MAC spoofing (probably SNMP hooks, etc.).

REMEDATION: If possible, use static IP addresses for the IP Phones. This will remove the necessity of using a DHCP server. Further, using a state based intrusion detection system can filter out DHCP server packets from IP Phone ports, allowing this traffic only from the legitimate server.

TFTP Server Insertion Attack

It is possible to change the configuration of a target phone by exploiting the TFTP response race when the IP phone is resetting. A rogue TFTP server can supply spurious

information before the legitimate server is able to respond to a request. This attack allows an attacker to change the configuration of an IP Phone.

REMEDIATION: Using a state based intrusion detection system can filter out DHCP server packets from IP Phone ports, allowing such traffic only from the legitimate server. Organizations looking to deploy VoIP systems should look for IP Phone instruments that can download signed binary files.

Availability and Denial of Service

Availability refers to the notion that information and services be available for use when needed. Availability is the most obvious risk for a switch. Attacks exploiting vulnerabilities in the switch software or protocols may lead to deterioration or even denial of service or functionality of the switch. For example: if unauthorized access can be established to any branch of the communication channel (such as a CCS link or a TCP/IP link), it may be possible to flood the link with bogus messages causing severe deterioration (possibly denial) of service. A voice over IP system may have additional vulnerabilities with Internet connections. Because intrusion detection systems fail to intercept a significant percentage of Internet based attacks, attackers may be able to bring down VoIP systems by exploiting weaknesses in Internet protocols and services.

Any network may be vulnerable to denial of service attacks, simply by overloading the capacity of the system. With VoIP the problem may be especially severe, because of its sensitivity to packet loss or delay.

CPU Resource Consumption Attack without any account information.

An attacker with remote terminal access to the server may be able to force a system restart (shutdown all/restart all) by providing the maximum number of characters for the login and password buffers multiple times in succession. Additionally, IP Phones may reboot as a result of this attack.

In addition to producing a system outage, the restart may not restore uncommitted changes or, in some cases, may restore default passwords, which would introduce intrusion vulnerabilities.

REMEDIATION: The deployment of a firewall disallowing connections from unnecessary or unknown network entities is the first step to overcoming this problem. However, there is still the opportunity for an attacker to spoof his MAC and IP address, circumventing the firewall protection.

Default Password Vulnerability

It is common for switches to have a default login/password set, e.g., admin/admin, or root/root. Similarly, VoIP telephones often have default keypad sequences that can be used to unlock and modify network information.

This vulnerability would allow an attacker to control the topology of the network remotely, allowing for not only complete denial of service to the network, but also a port mirroring attack to the attacker's location, giving the ability to intercept any other conversations taking place over the same switch. Further, the switch may have a web server interface, providing an attacker with the ability to disrupt the network without advance knowledge of switch operations and commands. In most systems, telephones download their configuration data on startup using TFTP or similar protocols. The configuration specifies the IP addresses for Call Manager nodes, so an attacker could substitute another IP address pointing to a call manager that would allow eavesdropping or traffic analysis.

REMEDIATION: Changing the default password is crucial. Moreover, the graphical user interface should be disabled to prevent the interception of plaintext administration sessions.

Exploitable software flaws

Like other types of software, VoIP systems have been found to have vulnerabilities due to buffer overflows and improper packet header handling. These flaws typically occur because the software is not validating critical information properly. For example, a short integer may be used as a table index without checking whether the parameter passed to the function exceeds 32,767, resulting in invalid memory accesses or crashing of the system.

Exploitable software flaws typically result in two types of vulnerabilities: denial of service or revelation of critical system parameters. Denial of service can often be implemented remotely, by passing packets with specially constructed headers that cause the software to fail. In some cases the system can be crashed, producing a memory dump in which an intruder can find IP addresses of critical system nodes, passwords, or other security-relevant information. In addition, buffer overflows that allow the introduction of malicious code have been found in VoIP software, as in other applications.

REMEDIATION: These problems require action from the software vendor, and distribution of patches to administrators. Intruders monitor announcements of vulnerabilities, knowing that many organizations require days or weeks to update their software. Regular checking for software updates and patches is essential to reducing these vulnerabilities. Automated patch handling can assist in reducing the window of opportunity for intruders to exploit known software vulnerabilities.

Account Lockout Vulnerability

An attacker will be able to provide several incorrect login attempts at the telnet prompt until the account becomes locked out. (This problem is common to most password-protected systems, because it prevents attackers from repeating login attempts until the correct password is found by trying all possible combinations.)

The account is unable to connect to the machine for the set lockout time.

REMEDIATION: If remote access is not available, this problem can be solved with physical access control.

NIST Recommendations.

Because of the integration of voice and data in a single network, establishing a secure VoIP and data network is a complex process that requires greater effort than that required for data-only networks. In particular, start with these general guidelines, recognizing that practical considerations, such as cost or legal requirements, may require adjustments for the organization:

1. Develop appropriate network architecture.

- Separate voice and data on logically different networks if feasible. Different subnets with separate RFC 1918 address blocks should be used for voice and data traffic, with separate DHCP servers for each, to ease the incorporation of intrusion detection and VoIP firewall protection at the voice gateway, which interfaces with the PSTN, disallow H.323, SIP, or other VoIP protocols from the data network. Use strong authentication and access control on the voice gateway system, as with any other critical network component. Strong authentication of clients towards a gateway often presents difficulties, particularly in key management. Here, access control mechanisms and policy enforcement may help.
- A mechanism to allow VoIP traffic through firewalls is required. There are a variety of protocol dependent and independent solutions, including application level gateways (ALGs) for VoIP protocols, Session Border Controllers, or other standards-based solutions when they mature.
- Stateful packet filters can track the state of connections, denying packets that are not part of a properly originated call. (This may not be practical when multimedia protocol inherent security or lower layer security is applied, e.g., H.235 Annex D for integrity provision or TLS to protect SIP signaling).
- Use IPsec or Secure Shell (SSH) for all remote management and auditing access. If practical, avoid using remote management at all and do IP PBX access from a physically secure system.
- If performance is a problem, use encryption at the router or other gateway, not the individual endpoints, to provide for IPsec tunneling. Since some VoIP endpoints are not computationally powerful enough to perform encryption, placing this burden at a central point ensures all VoIP traffic emanating from the enterprise network has been encrypted. Newer IP phones are able to provide Advanced Encryption System (AES) encryption at reasonable cost. Note that Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, is applicable to all Federal agencies that use cryptographic-based security systems to protect sensitive information in computer

and telecommunication systems (including voice systems) as defined in Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104-106.

2. Ensure that the organization has examined and can acceptably manage and mitigate the risks to their information, system operations, and continuity of essential operations when deploying VoIP systems.

VoIP can provide more flexible service at lower cost, but there are significant tradeoffs that must be considered. VoIP systems can be expected to be more vulnerable than conventional telephone systems, in part because they are tied in to the data network, resulting in additional security weaknesses and avenues of attack (see VoIP Risks, Threats, and Vulnerabilities section for more detailed discussion of vulnerabilities of VoIP and their relation to data network vulnerabilities).

Confidentiality and privacy may be at greater risk in VoIP systems unless strong controls are implemented and maintained. An additional concern is the relative instability of VoIP technology compared with established telephony systems. Today, VoIP systems are still maturing and dominant standards have not emerged. This instability is compounded by VoIP's reliance on packet networks as a transport medium. The public switched telephone network is ultra-reliable. Internet service is generally much less reliable, and VoIP cannot function without Internet connections, except in the case of large corporate or other users who may operate a private network. Essential telephone services, unless carefully planned, deployed, and maintained, will be at greater risk if based on VoIP.

3. Special consideration should be given to E-911 emergency services communications, because E-911 automatic location service is not available with VoIP in some cases.

Unlike traditional telephone connections, which are tied to a physical location, VoIP's packet switched technology allows a particular number to be anywhere. This is convenient for users, because calls can be automatically forwarded to their locations. But the tradeoff is that this flexibility severely complicates the provision of E-911 service, which normally provides the caller's location to the 911 dispatch office. Although most VoIP vendors have workable solutions for E-911 service, government regulators and vendors are still working out standards and procedures for 911 services in a VoIP environment. Agencies must carefully evaluate E-911 issues in planning for VoIP deployment.

4. Agencies should be aware that physical controls are especially important in a VoIP environment and deploy them accordingly.

Unless the VoIP network is encrypted, anyone with physical access to the office LAN could potentially connect network monitoring tools and tap into telephone conversations. Although conventional telephone lines can also be monitored when physical access is obtained, in most offices there are many more points to connect with a LAN without arousing suspicion. Even if encryption is used, physical access to VoIP servers and gateways may allow an attacker to do traffic analysis (i.e., determine which parties are communicating). Agencies therefore should ensure that adequate physical security is in place to restrict access to VoIP network components. Physical security measures, including barriers, locks, access control systems, and guards, are the first line of defense. Agencies must make sure that the proper physical countermeasures are in place to mitigate some of

the biggest risks such as insertion of sniffers or other network monitoring devices. Otherwise, practically speaking this means that installation of a sniffer could result in not just data but all voice communications being intercepted.

5. VoIP-ready firewalls and other appropriate protection mechanisms should be employed. Agencies must enable, use, and routinely test the security features that are included in VoIP systems.

Because of the inherent vulnerabilities (e.g. susceptibility to packet sniffing) when operating telephony across a packet network, VoIP systems incorporate an array of security features and protocols. Organization security policy should ensure that these features are used. In particular, firewalls designed for VoIP protocols are an essential component of a secure VoIP system.

6. If practical, “softphone” systems, which implement VoIP using an ordinary PC with a headset and special software, should not be used where security or privacy are a concern.

Worms, viruses, and other malicious software are extraordinarily common on PCs connected to the internet, and very difficult to defend against. Well-known vulnerabilities in web browsers make it possible for attackers to download malicious software without a user’s knowledge, even if the user does nothing more than visit a compromised web site. Malicious software attached to email messages can also be installed without the user’s knowledge, in some cases even if the user does not open the attachment. These vulnerabilities result in unacceptably high risks in the use of “softphones”, for most applications. In addition, because PCs are necessarily on the data network, using a softphone system conflicts with the need to separate voice and data networks to the greatest extent practical.

7. If mobile units are to be integrated with the VoIP system, use products implementing WiFi Protected Access (WPA), rather than 802.11 Wired Equivalent Privacy (WEP).

The security features of 802.11 WEP provide little or no protection because WEP can be cracked with publicly available software. The more recent WiFi Protected Access (WPA), a snapshot of the ongoing 802.11i standard, offers significant improvements in security, and can aid the integration of wireless technology with VoIP. NIST strongly recommends that the WPA (or WEP if WPA is unavailable) security features be used as part of an overall defense-in-depth strategy. Despite their weaknesses, the 802.11 security mechanisms can provide a degree of protection against unauthorized disclosure, unauthorized network access, or other active probing attacks. However, the Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, is mandatory and binding for Federal agencies that have determined that certain information must be protected via cryptographic means. As currently defined, neither WEP nor WPA meets the FIPS 140-2 standard. In these cases, it will be necessary to employ higher level cryptographic protocols and applications such as secure shell (SSH), Transport Level Security (TLS) or Internet Protocol Security (IPsec) with FIPS 140-2 validated cryptographic modules and associated algorithms to protect information, regardless of whether the nonvalidated data link security protocols are used.

8. Carefully review statutory requirements regarding privacy and record retention with competent legal advisors.

Although legal issues regarding VoIP are beyond the scope of this document, readers should be aware that laws and rulings governing interception or monitoring of VoIP lines, and retention of call records, may be different from those for conventional telephone systems. Agencies should review these issues with their legal advisors. See Section 2.5 for more on these issues.

G.3 Cloud Computing

Cloud Computing

Purpose:

This paper is provided to define and describe cloud computing, discuss CJIS Security Policy (CSP) compliance, detail security and privacy, and provide general recommendations.

Attribution:

- NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing (Dec. 2011)
- NIST SP 800-145, the NIST Definition of Cloud Computing (Sept. 2011)
- NIST SP 800-146, Cloud Computing Synopsis and Recommendations (May 2011)
- CJIS Security Policy, Version 5.0

Definitions and Terms:

Cloud computing – A distributed computing model that permits on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services), software, and information.

Cloud subscriber – A person or organization that is a customer of a cloud

Cloud client – A machine or software application that accesses a cloud over a network connection, perhaps on behalf of a subscriber

Cloud provider – An organization that provides cloud services

Summary:

With many law enforcement agencies looking for ways to attain greater efficiency while grappling with reduced budgets, the idea of cloud computing to maintain data and applications is a viable business solution. But the unique security and legal characteristics of law enforcement agencies means any migration to cloud services may be challenging. Anytime the security of information and transactions must be maintained, as it must be with access to the FBI's CJIS systems and the protection of Criminal Justice Information (CJI), security and policy compliance concerns are bound to arise.

Cloud computing has become a popular and sometimes contentious topic of discussion for both the private and public sectors. This is in part because of the difficulty in describing cloud computing in general terms, because it is not a single kind of system. The “cloud” spans a spectrum of underlying technologies, configuration possibilities, service and deployment models. Cloud computing offers the ability to conveniently rent access to fully featured applications, software development and deployment environments, and computing infrastructure assets - such as network-accessible data storage and processing from a cloud service provider.

One of the benefits of cloud computing is the ability to outsource many of the technical functions agencies may not want to perform for various reasons. Ultimately, the move to cloud computing is a business and security risk decision in which the following relevant factors are given proper consideration:

- readiness of existing applications for cloud deployment
- transition costs
- life-cycle costs
- maturity of service orientation in existing infrastructure
- security and privacy requirements – federal, state, and local

Achieving CJIS Security Policy Compliance:

The question that is often asked is, “Can an Agency be compliant with the CJIS Security Policy and also cloud compute?”

Because the CJIS Security Policy is device and architecture independent (per CSP Section 2.2), the answer is yes, and this can be accomplished— assuming the vendor of the cloud technology is able to meet the existing requirements of the CJIS Security Policy.

There are security challenges that must be addressed if CJI is to be sent into or through, stored within, or accessed from the cloud.

Admittedly, the existing CJIS Security Policy requirements may be difficult for some cloud-computing vendors due to the sheer numbers and the geographic disbursement of their personnel; however, the requirements aren’t new to vendors serving the criminal justice community and many vendors have been successfully meeting the Policy requirements for years. Even so, they are the minimum security requirements which will provide an acceptable level of assurance that law enforcement and personally identifiable information (PII) will be protected when shared with other law enforcement agencies across the nation.

General CJIS Security Policy Applicability Questions

Before tackling these challenges, the cloud subscriber should first be aware of what security and legal requirements they are subject to prior to entering into any agreement with a cloud provider. Asking the following general questions will help frame the process of determining compliance with the existing requirements of the CJIS Security Policy.

- Will access to Criminal Justice Information (CJI) within a cloud environment fall within the category of remote access? (5.5.6 Remote Access)
- Will advanced authentication (AA) be required for access to CJI within a cloud environment? (5.6.2.2 Advanced Authentication, 5.6.2.2.1 Advanced Authentication Policy and Rationale)
- Does/do any cloud service provider's datacenter(s) used in the transmission or storage of CJI meet all the requirements of a physically secure location? (5.9.1 Physically Secure Location)
- Are the encryption requirements being met? (5.10.1.2 Encryption)
 - Who will be providing the encryption as required in the CJIS Security Policy (client or cloud service provider)? *Note: individuals with access to the keys can decrypt the stored files and therefore have access to unencrypted CJI.*
 - Is the data encrypted while at rest and in transit?
- What are the cloud service provider's incident response procedures? (5.3 Policy Area 3: Incident Response)
 - Will the cloud subscriber be notified of any incident?
 - If CJI is compromised, what are the notification and response procedures?
- Is the cloud service provider a private contractor/vendor?
 - If so, they are subject to the same screening and agreement requirements as any other private contractors hired to handle CJI? (5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum; 5.12.1.2 Personnel Screening for Contractors and Vendors)
- Will the cloud service provider allow the CSA and FBI to conduct compliance and security audits? *Note: Cloud facilities such as datacenters in which CJI will be stored or processed should be audited as would any other datacenter housing and processing CJI.* (5.11.1 Audits by the FBI CJIS Division; 5.11.2 Audits by the CSA)

- How will event and content logging be handled? (5.4 Policy Area 4, Auditing and Accountability)
 - Will the cloud service provider handle the events and content logging required by the CJIS Security Policy and provide that upon request?
 - What are the cloud service provider's responsibilities with regard to media protection and destruction? (5.8 Policy Area 8: Media Protection)

Ultimately, the goal is to remain committed to using technology in its information sharing processes, but not at the sacrifice of the security of the information with which it has been entrusted. As stated in the CJIS Security Policy, device and architecture independence permits the use of cloud computing, but the security requirements do not change.

Cloud Utilization Scenarios

1. Encrypted CJI in a Cloud Environment—Key Management Control, Security Awareness Training, and Personnel Controls

Prior to permitting CJI to be stored or traverse through a cloud environment, the agency should ensure proper encryption key management control procedures are implemented to determine who has access and control over the encryption keys. Proper key management control is vital to CJI security as those individuals (agency or cloud employees) with access to the keys can decrypt the stored files, and therefore, have unescorted access to unencrypted CJI. This means all those individuals must be subjected to security awareness training (CJIS Security Policy section 5.2) and must meet personnel security (CJIS Security Policy Section 5.12) requirements as individuals with unescorted access to unencrypted CJI.

Note: As a best security practice, the CJIS ISO Program does not recommend allowing the cloud service provider access to the encryption keys used to protect CJI. However, it may not always be reasonable to expect the agency, criminal justice or noncriminal justice, to accomplish this task.

- a. Scenario 1—Agency Stores CJI in a Cloud:

A CJA stores encrypted CJI (Backup files and drives) in a cloud service provider's environment. To access CJI, the agency will extract the CJI from the cloud to its local machine, and then decrypt the CJI. The CJI is processed, re-encrypted, and then re-uploaded to the cloud environment for storage. In this scenario, the agency always encrypts the CJI prior to placing it in the cloud and only authorized users of the agency have access to the encryption keys. Since the agency maintains the encryption keys, the cloud service provider employees would not need to undergo fingerprint-based background checks, nor have security awareness training. These requirements are negated, because only authorized personnel with access to the keys have the ability to view this CJI in an unencrypted form.

- b. Scenario 2—Agency Accesses CJI While in a Cloud:

A CJA stores CJI (files and drives) in a cloud service provider's environment, but as part of daily operations authorized users will remotely access the encrypted CJI in the cloud. The user will decrypt the CJI while it is in the cloud's virtual environment, process the data, and then re-encrypt the data prior to ending the remote session. The agency maintains the keys and the cloud service provider does not have access to the encryption keys. However, since the CJI is decrypted within the cloud's virtual environment, any administrative personnel employed by the cloud provider having the ability to access the virtual environment must be identified and subjected to security awareness training and personnel security controls as described in the CJIS Security Policy.

c. Scenario 3–CJI Impact from a Cloud Datacenter Critical Systems Crash–Core Dump² Recovery:

A CJA utilizes a cloud service provider (IaaS or PaaS) to store CJI and remotely accesses the environment to process CJI. During normal operation, the cloud provider experiences systems outages within the datacenter in which CJI is processed and stored. The cloud provider's administrators need to repair the systems and restore service using data from a core dump to return to normal operations. The cloud service provider as part of the Service Level Agreement (SLA) with the CJA has been authorized to maintain the encryption keys in order respond to such an event. The cloud administrators with such access have underwent fingerprint-based background checks and security awareness training. This allows the cloud administrators to decrypt CJI so that it is written to the core dump files for restoration following the system outage. CJI, however, is encrypted at all times except when part of the core dump files. As part of the SLA, the cloud service provider has agreed to treat the core dump files as CJI to ensure all protection are in place in compliance with the CJIS Security Policy.

Note: Writing encrypted data to a core dump corrupts the data and makes it unusable because the key no longer decrypts the data. This is problematic when attempting to recover encrypted data written to a core dump. The CJA could have ensured the cloud provider exclude encrypted data (CJI) from the core dump, but chose against it.

The Cloud Model Explained:

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

² Core Dump - A file of a computer's documented memory of when a program or computer crashed. The file consists of the recorded status of the working memory at an explicit time, usually close to when the system crashed or when the program ended atypically as it presents the risk that the system failure would ensure the loss of the encrypted data.

The cloud model as defined by NIST consists of five essential characteristics, offers the option of three service models, and may be deployed via any of four deployment models as shown in Figure 1 below:

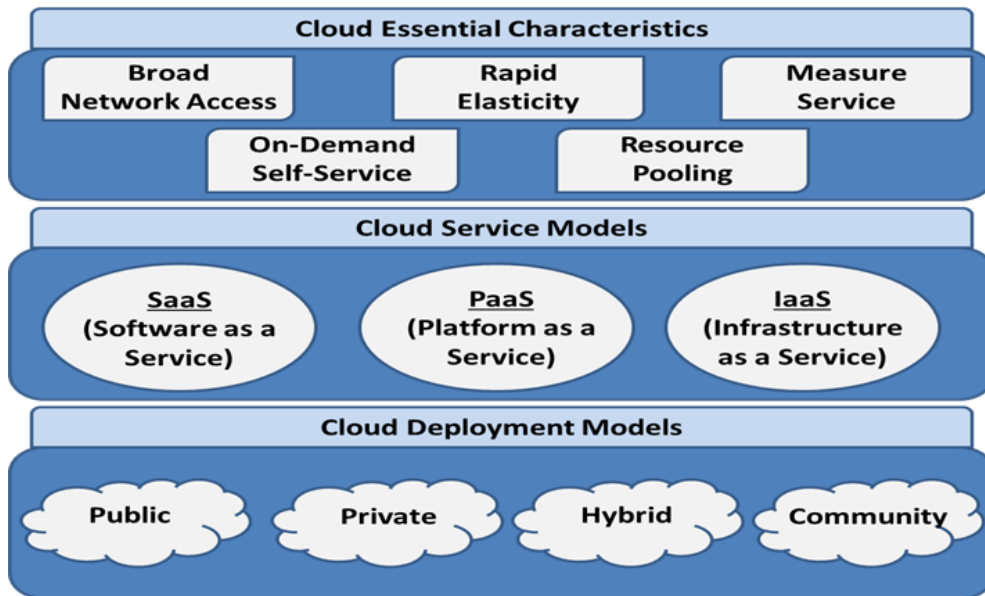


Figure 1 - Visual Depiction of the NIST Cloud Computing Definition

Essential Characteristics:

On-demand self-service

A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access

Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling

The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in which the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction

(e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

Rapid elasticity

Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured service

Cloud systems automatically control and optimize resource use by leveraging a metering capability* at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

** Typically this is done on a pay-per-use or charge-per-use basis.*

Deployment Models:

Private cloud

The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Community cloud

The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud

The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud

The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Service Models:

Software as a Service (SaaS)

This model provides the consumer the capability to use the provider's applications running on a cloud infrastructure*.

** A cloud infrastructure is the collection of hardware and software that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually the abstraction layer sits above the physical layer.*

The SaaS service model is often referred to as “Software deployed as a hosted service and accessed over the Internet.”

The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface.

When using the SaaS service model it should be understood that the consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Platform as a Service (PaaS)

This model provides the consumer the capability to deploy consumer-created or acquired applications* created using programming languages, libraries, services, and tools supported by the provider onto the cloud infrastructure.

** This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources.*

When using the PaaS service model the consumer may have control over the deployed applications and possibly configuration settings for the application-hosting environment, but does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage.

Infrastructure as a Service (IaaS)

This model provides the consumer the capability to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, including operating systems and applications.

When using the IaaS service model the consumer may have control over operating systems, storage, and deployed applications; and possibly limited control of select

networking components (e.g., host firewalls), but does not manage or control the underlying cloud infrastructure.

Key Security and Privacy Issues:

Although the emergence of cloud computing is a recent development, insights into critical aspects of security can be gleaned from reported experiences of early adopters and also from researchers analyzing and experimenting with available cloud provider platforms and associated technologies. The sections below highlight privacy and security-related issues that are believed to have long-term significance for public cloud computing and, in many cases, for other cloud computing service models.

Because cloud computing has grown out of an amalgamation of technologies, including service oriented architecture, virtualization, Web 2.0, and utility computing, many of the privacy and security issues involved can be viewed as known problems cast in a new setting. The importance of their combined effect in this setting, however, should not be discounted. Public cloud computing does represent a thought-provoking paradigm shift from conventional norms to an open organizational infrastructure—*at the extreme, displacing applications from one organization's infrastructure to the infrastructure of another organization, where the applications of potential adversaries may also operate.*

Governance

Governance implies control and oversight by the organization over policies, procedures, and standards for application development and information technology service acquisition, as well as the design, implementation, testing, use, and monitoring of deployed or engaged services. With the wide availability of cloud computing services, lack of organizational controls over employees engaging such services arbitrarily can be a source of problems. While cloud computing simplifies platform acquisition, it doesn't alleviate the need for governance; instead, it has the opposite effect, amplifying that need.

Dealing with cloud services requires attention to the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met. Ensuring systems are secure and risk is managed is challenging in any environment and even more daunting with cloud computing. Audit mechanisms and tools should be in place to determine how data is stored, protected, and used, to validate services, and to verify policy enforcement. A risk management program should also be in place that is flexible enough to deal with the continuously evolving and shifting risk landscape.

Compliance

Compliance refers to an organization's responsibility to operate in agreement with established laws, regulations, standards, and specifications. Various types of security and privacy laws and regulations exist within different countries at the national, state, and local levels, making compliance a potentially complicated issue for cloud computing.

Law and Regulations

Cloud providers are becoming more sensitive to legal and regulatory concerns, and may be willing to commit to store and process data in specific jurisdictions and apply required safeguards for security and privacy. However, the degree to which they will accept liability in their service agreements, for exposure of content under their control, remains to be seen. Even so, organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf.

Data Location

One of the most common compliance issues facing an organization is data location. A characteristic of many cloud computing services is that data is stored redundantly in multiple physical locations and detailed information about the location of an organization's data is unavailable or not disclosed to the service consumer. This situation makes it difficult to ascertain whether sufficient safeguards are in place and whether legal and regulatory compliance requirements are being met. External audits and security certifications can alleviate this issue to some extent, but they are not a panacea.

When information crosses borders, the governing legal, privacy, and regulatory regimes can be ambiguous and raise a variety of concerns. Consequently, constraints on the trans-border flow of sensitive data, as well as the requirements on the protection afforded the data, have become the subject of national and regional privacy and security laws and regulations.

Electronic Discovery

The capabilities and processes of a cloud provider, such as the form in which data is maintained and the electronic discovery-related tools available, affect the ability of the organization to meet its obligations in a cost effective, timely, and compliant manner. A cloud provider's archival capabilities may not preserve the original metadata as expected, causing spoliation (i.e., the intentional, reckless, or negligent destruction, loss, material alteration, or obstruction of evidence that is relevant to litigation), which could negatively impact litigation.

Trust

Under the cloud computing paradigm, an organization relinquishes direct control over many aspects of security and privacy, and in doing so, confers a high level of trust onto the cloud provider. At the same time, federal agencies have a responsibility to protect information and information systems commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction, regardless of whether the information is collected or maintained by or on behalf of the agency; or whether the information systems are used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency

Insider Access

Data processed or stored outside the physical confines of an organization, its firewall, and other security controls bring with it an inherent level of risk. The insider security threat is a well-known issue for most organizations. Incidents may involve various types of fraud, sabotage of information resources, and theft of sensitive information.

Data Ownership

The organization's ownership rights over the data must be firmly established in the service contract to enable a basis for trust and privacy of data. The continuing controversy over privacy and data ownership rights for social networking users illustrates the impact that ambiguous terms can have on the parties involved.

Ideally, the contract should state clearly that the organization retains exclusive ownership over all its data; that the cloud provider acquires no rights or licenses through the agreement, including intellectual property rights or licenses, to use the organization's data for its own purposes; and that the cloud provider does not acquire and may not claim any interest in the data due to security. For these provisions to work as intended, the terms of data ownership must not be subject to unilateral amendment by the cloud provider.

Visibility

Continuous monitoring of information security requires maintaining ongoing awareness of security controls, vulnerabilities, and threats to support risk management decisions. Transition to public cloud services entails a transfer of responsibility to the cloud provider for securing portions of the system on which the organization's data and applications operate.

Ancillary Data

While the focus of attention in cloud computing is mainly on protecting application data, cloud providers also hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks.

Risk Management

Assessing and managing risk in systems that use cloud services can be a challenge. With cloud-based services, some subsystems or subsystem components fall outside of the direct control of a client organization. Many organizations are more comfortable with risk when they have greater control over the processes and equipment involved. Establishing a level of trust about a cloud service is dependent on the degree of control an organization is able to exert on the provider to provision the security controls necessary to protect the organization's data and applications, and also the evidence provided about the effectiveness of those controls. Ultimately, if the level of trust in the service falls below expectations and the organization is unable to employ compensating controls, it must either reject the service or accept a greater degree of risk.

Architecture

The architecture of the software and hardware used to deliver cloud services can vary significantly among public cloud providers for any specific service model. It is important to understand the technologies the cloud provider uses to provision services and the implications the technical controls involved have on security and privacy of the system throughout its lifecycle. With such information, the underlying system architecture of a cloud can be decomposed and mapped to a framework of security and privacy controls that can be used to assess and manage risk.

Identity and Access Management

Data sensitivity and privacy of information have become increasingly an area of concern for organizations. The identity proofing and authentication aspects of identity management entail the use, maintenance, and protection of PII collected from users. Preventing unauthorized access to information resources in the cloud is also a major consideration. One recurring issue is that the organizational identification and authentication framework may not naturally extend into a public cloud and extending or changing the existing framework to support cloud services may prove difficult.

Software Isolation

High degrees of multi-tenancy over large numbers of platforms are needed for cloud computing to achieve the envisioned flexibility of on-demand provisioning of reliable services and the cost

benefits and efficiencies due to economies of scale. Regardless of the service model and multi-tenant software architecture used, the computations of different consumers must be able to be carried out in isolation from one another, mainly through the use of logical separation mechanisms.

Data Protection

Data stored in a public cloud typically resides in a shared environment collocated with data from other customers. Organizations placing sensitive and regulated data into a public cloud, therefore, must account for the means by which access to the data is controlled and the data is kept secure. Similar concerns exist for data migrated within or between clouds.

Value Concentration

Having data collocated with that of an organization with a high threat profile could also lead to a denial of service, as an unintended casualty from an attack targeted against that organization. Similarly, side effects from a physical attack against a high profile organization's cloud-based resources are also a possibility. For example, over the years, facilities of the Internal Revenue Service have attracted their share of attention from would-be attackers.

Data Isolation

Database environments used in cloud computing can vary significantly. Accordingly, various types of multi-tenant arrangements exist for databases. Each arrangement pools resources differently, offering different degrees of isolation and resource efficiency. Regardless of implementation decision, data must be secured while at rest, in transit, and in use, and access to the data must be controlled.

Data Sanitization

The data sanitization practices that a cloud provider implements have obvious implications for security. Sanitization involves the expunging of data from storage media by overwriting, degaussing, or other means, or the destruction of the media itself, to prevent unauthorized disclosure of information. Data sanitization also applies to backup copies made for recovery and restoration of service and residual data remaining upon termination of service.

In a public cloud computing environment, data from one consumer is physically collocated (e.g., in an IaaS data store) or commingled (e.g., in a SaaS database) with the data of other consumers, which can complicate matters. Service agreements should stipulate sufficient measures that are taken to ensure data sanitization is performed appropriately throughout the system lifecycle.

Encryption

Client end-to-end encryption (e.g. encryption/decryption occurs on the law enforcement controlled client prior to data entering the cloud and decryption occurs only on the client device after encrypted data is removed from the cloud service) with cryptographic keys managed solely by law enforcement would prevent exposure of sensitive data.

- May cause significant cloud service functionality limitations on available service types made available for sensitive data. This may also increase expenses to cover key items, such as key management and client software. Additionally, a number of specific SLA or contract clauses may be necessary for the implementation of client end-to end encryption.

Use of cloud services without end-to-end encryption implemented by the client is another option that would require cloud service provider participation in the encryption of data.

- This would require at least some cloud provider personnel to undergo personnel background screening and training.
- Specialized Service Level Agreements (SLA) and/or contractual clauses would be necessary to identify those personnel that may have access to unencrypted, sensitive data.
- Conducting the analysis and gaining approval of particular cloud service implementations not utilizing end-to-end encryption for sensitive law enforcement data may be costly and time consuming due to the high degree of technical complexity.

Availability

In simple terms, availability is the extent to which an organization's full set of computational resources is accessible and usable. Denial of service attacks, equipment outages, and natural disasters are all threats to availability. The concern is that most downtime is unplanned and can impact the mission of the organization. Some examples of unplanned service interruptions that cause concerns are:

- Temporary Outages
- Prolonged and Permanent Outages
- Denial of Service

Incident Response

The complexity of a cloud service can obscure recognition and analysis of incidents. Revising an organization's incident response plan to address differences between the organizational computing environment and a cloud computing environment is an important, but easy-to-overlook prerequisite to transitioning applications and data.

Data Availability

The availability of relevant data from event monitoring is essential for timely detection of security incidents. Cloud consumers are often confronted with extremely limited capabilities for detection of incidents in public cloud environments. The situation varies among cloud service models and cloud providers. For example, PaaS providers typically do not make event logs available to consumers, who are then left mainly with event data from self-deployed applications (e.g., via application logging). Similarly, SaaS consumers are completely dependent upon the cloud provider to provide event data such as activity logging, while IaaS consumers control more of the information stack and have access to associated event sources.

Incident Analysis and Resolution

An analysis to confirm the occurrence of an incident or determine the method of exploit needs to be performed quickly and with sufficient detail of documentation and care to ensure that traceability and integrity is maintained for subsequent use, if needed (e.g., a forensic copy of incident data for legal proceedings). Issues faced by cloud consumers when performing incident analysis include lack of detailed information about the architecture of the cloud relevant to an incident, lack of information about relevant event and data sources held by the cloud provider, ill-defined or vague incident handling responsibilities stipulated for the cloud provider, and limited capabilities for gathering and preserving pertinent data sources as evidence. Understanding and negotiating the provisions and procedures for incident response should be done before entering into a service contract, rather than as an afterthought.

General Recommendations:

A number of significant security and privacy issues were covered in the previous subsections. Table 1 summarizes those issues and related recommendations for organizations to follow when planning, reviewing, negotiating, or initiating a public cloud service outsourcing arrangement.

Table 1: Security and Privacy Issue Areas and Recommendations

Areas	Recommendations
Governance	<ul style="list-style-type: none"> Extend organizational practices pertaining to the policies, procedures, and standards used for application development and service provisioning in the cloud, as well as the design, implementation, testing, use, and monitoring of deployed or engaged services. Put in place audit mechanisms and tools to ensure organizational practices are followed throughout the system lifecycle.
Compliance	<ul style="list-style-type: none"> Understand the various types of laws and regulations that impose security and privacy obligations on the organization and potentially impact cloud computing initiatives, particularly those involving data location, privacy and security controls, records management, and electronic discovery requirements. Review and assess the cloud provider’s offerings with respect to the organizational requirements to be met and ensure that the contract terms adequately meet the requirements. Ensure that the cloud provider’s electronic discovery capabilities and processes do not compromise the privacy or security of data and applications.
Trust	<ul style="list-style-type: none"> Ensure that service arrangements have sufficient means to allow visibility into the security and privacy controls and processes employed by the cloud provider, and their performance over time. Establish clear, exclusive ownership rights over data. Institute a risk management program that is flexible enough to adapt to the constantly evolving and shifting risk landscape for the lifecycle of the system. Continuously monitor the security state of the information system to support on-going risk management decisions.
Architecture	<ul style="list-style-type: none"> Understand the underlying technologies that the cloud provider uses to provision services, including the implications that the technical controls involved have on the security and privacy of the system, over the full system lifecycle and across all system components.
Identity and Access Management	<ul style="list-style-type: none"> Ensure that adequate safeguards are in place to secure authentication, authorization, and other identity and access management functions, and are suitable for the organization.
Software Isolation	<ul style="list-style-type: none"> Understand virtualization and other logical isolation techniques that the cloud provider employs in its multi-tenant software architecture, and assess the risks involved for the organization.
Data Protection	<ul style="list-style-type: none"> Evaluate the suitability of the cloud provider’s data management solutions for the organizational data concerned and the ability to control access to data, to secure data while at rest, in transit, and in use, and to sanitize data.

- Take into consideration the risk of collating organizational data with that of other organizations whose threat profiles are high or whose data collectively represent significant concentrated value.
- Fully understand and weigh the risks involved in cryptographic key management with the facilities available in the cloud environment and the processes established by the cloud provider.

Availability

- Understand the contract provisions and procedures for availability, data backup and recovery, and disaster recovery, and ensure that they meet the organization’s continuity and contingency planning requirements.
- Ensure that during an intermediate or prolonged disruption or a serious disaster, critical operations can be immediately resumed, and that all operations can be eventually reinstated in a timely and organized manner.

Incident Response

- Understand the contract provisions and procedures for incident response and ensure that they meet the requirements of the organization.
 - Ensure that the cloud provider has a transparent response process in place and sufficient mechanisms to share information during and after an incident.
 - Ensure that the organization can respond to incidents in a coordinated fashion with the cloud provider in accordance with their respective roles and responsibilities for the computing environment.
-

G.4 Mobile Appendix

Mobile Appendix

Introduction

Mobile devices present a unique security challenge with regard to the correct application of CJIS Security Policy requirements. This appendix is intended to provide best practices based on industry standards and on methods to achieve policy compliance in mobile device employment scenarios. The technical methods used to achieve compliance with CJIS Security Policy will typically be different within the mobile environment than those used in fixed locations. Many of the security features and capabilities inherited by endpoint devices from the fixed environment are either not present or present in a different form in the mobile environment. Additionally, the basic technologies used in some types of mobile devices may adequately fulfill some of the CJIS Security Policy requirements which would require additional software or added features in a traditional fixed computing environment. Due to the complexity and rapid evolution of the mobile environment, this Appendix will remain as device and vendor agnostic as practical, however certain key requirements for specific mobile operating systems will be identified for the major mobile operating systems (e.g. Apple iOS, Android) as the underlying technologies are fundamentally different and offer different levels of built-in compliance to CJIS Security Policy.

Sections within this appendix will provide recommendations regarding priorities and level of effort versus value of applying certain security controls in the mobile environment. These recommendations do not supersede or modify the requirements listed in the CJIS Security Policy, and are intended to describe the effect of inherent security functions and inherent device limitations in many mobile platforms that impact the application of policy elements in the mobile environment.

Mobile Device Risk Scenarios

There are multiple risk scenarios that may apply to mobile devices depending on the category of device (e.g. Laptop, Tablet, and 'Pocket sized' devices such as smartphones) and the methods of device connectivity (e.g. cellular service, WiFi + Cellular, WiFi only). Device category and method of connection define the technology types within the device which inherently affects the total level of compliance with CJIS Security Policy that can be obtained by the mobile device.

It is advisable for acquiring agencies to review the mobile device guidance in this Appendix prior to completing selection and acquisition of particular devices. Both the device category and connectivity methods installed and configured on the device will impact the overall risk scenario associated with the device and may significantly affect the effective cost to bring use of the device in compliance with the CJIS Security Policy. For instance, inclusion of cellular radios with the ability to remotely control a device significantly changes the risk scenario by allowing remote tracking, file deletion, and device management which could provide a higher level of CJIS Security Policy compliance than a WiFi only device that does not guarantee the ability to remotely manage the device. However, inclusion of cellular technology may significantly increase the initial device costs and incur ongoing subscription costs. Appropriate choices based on the intended use of the device along with the types and methods of Criminal Justice Information (CJI) data to be accessed could greatly reduce agency cost and enhance security.

Device Categories

This appendix defines risk levels for three categories of devices. Prior to reading individual sections of this Appendix, the agency should identify which device categories will apply to their employment scenario. If multiple categories of devices are employed, individual technical configurations and local policy will likely need to be defined for each category of device based on the risk inherent in the technical characteristics associated with each device category.

Laptop devices

The laptop device category includes mobile devices in a larger format that are transported either in a vehicle mount or a carrying case and include a monitor with attached keyboard. This includes all traditional laptop computers that utilize a ‘traditional’, full-featured operating system (e.g. Windows or a Linux variant). Also included in this category are ‘tablet’ type full-featured computers running a traditional full-featured operating system but without an attached keyboard. The main defining factor is the use of a full-featured operating system and a form factor too large to be carried in a pocket. In general, devices of this type connect via WiFi only, but may include an internal cellular access card in some cases.

The risks associated with this device type are similar to a standard desktop computer at the technical level, but are increased due to the potential to connect directly to the internet without the benefit of organizational network security layers (e.g. network firewall, IDS/IPS, network monitoring devices). There is also an increased risk of intentional device theft from vehicles or unsecure locations as these devices are too large to be carried on the authorized user’s body. There may be increased risk from the limited technical ability to wipe or track a lost/stolen device depending on the particular technical means used for remote device connectivity (e.g. cellular or WiFi).

In general, the technical configurations for compliance with most of the CJIS Security Policy that is accomplished via the operating system (e.g. auditing, access control, etc) will remain consistent with normal fixed location computing systems for laptop devices, but some functions may operate in an unexpected manner due to lack of constant connectivity. Thorough testing of applied security policy elements within the expected mobile environments will help ensure the applied policy configurations remain effective and appropriate when applied to mobile laptop devices.

NOTE: Some newer devices running multi-function operating systems (e.g. Windows 8 or similar multi-mode operating systems) may exhibit technical features associated with both laptop and tablet device categories based on their current operating mode which may be reconfigured by the user on demand. If this is the case, it will be necessary to assess and configure multiple operating modes to be compliant with CJIS Security Policy on the device, or restrict the operating mode to one category of operation.

Tablet devices

The tablet device category includes larger format devices transported via vehicle mount or portfolio sized carry case that typically consist of a touch screen without attached keyboard. These devices utilize a limited-feature operating system (e.g. Apple iOS, Google Android, Windows mobile) that is inherently more resistant than a traditional operating system to certain types of network based technical attacks due to the limited-feature sets. Additionally, limited functionality operating systems are designed specifically for the mobile environment where battery life and power efficiency are primary design drivers. This inherently limits the types of services that can

function effectively on the devices (e.g. traditional real-time anti-virus software) as the base operating system may not be designed to allow installed applications enhanced execution priority in the background and or the ability to examine the contents or communications associated within another application. However, this same design methodology significantly limits the vectors available for malware transmission and the device or application data actually accessible to malware if a device becomes infected.

Tablet devices will have different risks associated depending on the installed and configured methods for network access (e.g. ‘always on cellular’ vs. WiFi only). Physical risks associated with this category are similar to the laptop category for enhanced likelihood of intentional theft or device hijacking while unattended, while the technical risks are similar to the pocket device category.

Pocket devices/Handheld devices

The pocket/handheld device category is technically similar or identical to the tablet category and is primarily differentiated by device form factor. Pocket/handheld devices are characterized as having a limited functionality operating system and a small form factor intended for carry in a pocket or ‘holster’ attached to the body. The bulk of this category will be cellular ‘smartphones’ with integrated cellular data connectivity, however devices intended to be worn or carried on the body (e.g. portable fingerprint devices) may also be included in this category if they operate using a limited functionality operating system. Custom or specialty devices may meet the form factor distinction for this category, but operate using a full-feature operating system. In rare cases of this nature the employing agency should apply security guidance and principles in this appendix for both the laptop and pocket device categories.

Risks associated with this category are a reduced threat of theft to a stored devices (e.g. device left unattended in a vehicle) since these devices are typically carried continuously by the authorized user, but include a greater risk of temporary or permanent loss of control due to the device being misplaced by the authorized user.

Due to the installation of a limited functionality operating system, the technical threat to these devices via a network based attack is significantly lower than the laptop category, however, the threat of unauthorized access at the device level may be higher if the device is lost due to technical limits on multi-factor authentication to the operating system itself and practical limits to device passwords due to screen/software keyboard limitations.

NOTE: Data accessible on pocket or tablet devices simply through the entry of a single device PIN or password should not be considered secure due to the likelihood of enhanced password guessing based on fingerprints/smudges on the device touch screen. Any data stored on devices of these types should be protected within a separate secure container using Advanced Authentication.

Device Connectivity

There are three main categories of device connectivity that are associated with varying risk levels and threats to the devices. The Three categories are: Cellular Network Only (always on), WiFi Only (includes ‘on demand’ cellular), and Cellular (always on) + WiFi network. The risks associated with connectivity categories are general risks and may apply differently to any particular device at different points in its usage or lifecycle. Particular device configurations either through the operating system or a third-party mobile device management (MDM) system may be

able to significantly control and define which particular connectivity risks may be associated with a particular device.

Cellular Network Only (always on)

Cellular network connectivity is characterized by ‘always on’ network connection through the device internal radio to a cellular network provider. There is a reasonable assurance that devices with ‘always on’ cellular can be tracked, managed, or wiped remotely if lost or stolen. This will significantly reduce risks associated with loss of the device and attempted illicit access to the device. One important consideration for this risk category is characterization of the device as ‘always on’ or ‘on demand’. In effect the difference is typically a configuration setting, which in some cases may be changeable by the user. In particular most cellular smart phones contain ‘airplane’ mode settings that disable all internal radios allowing a user authenticated to the device operating system via password or personal identification number (PIN) to disable the cellular system. Access to this functionality may be disabled through the use of some MDM systems which would necessitate a complete power down of the device while carried on aircraft. Additionally, someone illicitly obtaining a device with properly configured password requirements and screen lock timeouts would be unlikely to guess the device password before the device was reported stolen in order for them to disable the cellular connection and prevent tracking or a remote wipe of the device.

Cellular networks do not allow for the same level of exposure of individual devices to random access from the internet. This significantly reduces the potential network based attack vectors that might reach a cellular connected device. The risk scenario in most cases from a network based attack would be similar to a device protected behind rudimentary network defenses (e.g. standard firewall but NOT advanced intrusion detection/prevention) Cellular device communications cannot typically be accessed by other ‘eavesdropping’ devices physically close to them without significant specialized equipment and can be considered well protected against network attacks below the nation/state level of technical capability by the hosting technical infrastructure and technology inherent in the device. However, network based attacks that utilize connections initiated by the user device may still succeed over the cellular infrastructure. For this reason, the technical protections inherent in the cellular infrastructure provide limited protection against user/device initiated actions (e.g. web surfing on a cellular connected web browser). Therefore, the protections provided by always on cellular connections are primarily in the ability to remotely access the mobile device for tracking or data deletion in case of device loss or compromise, which combined with a limited functionality device operating system, the protections are generally equivalent to a ‘personal firewall’ if properly configured and supported by a well-designed organizational infrastructure. However, that equivalency does not apply to full-featured operating systems connected through cellular infrastructure.

NOTE: It should be noted that a technically capable, intentional, thief knowingly obtaining an ‘always on’ cellular device for the purpose of data theft can physically disable the radio by utilizing a Faraday cage or similar external electromagnetic shield device while attempting to guess the device password. While technically possible these methods require specialized equipment and high technical expertise and would be very unlikely to be employed except for specifically targeted attacks. When always on cellular connectivity is combined with a robust incident reporting process and user training for rapid response to device loss or theft, the associated risks can be minimized.

WiFi only (includes ‘on-demand’ cellular)

WiFi only devices do not include cellular radios or include cellular radio that must be manually activated or ‘connected’ to the cellular network. They connect to the network or internet through WiFi ‘hotspots’ or external access points or manually to cellular networks. Some MDM or device configurations may be able to limit the types and specific WiFi access points the device can connect to, which may change the risk scenario of the device to a similar risk scenario as the Cellular Network Only scenario. However, if mobile devices are permitted (through technical and or policy decisions) to connect to any WiFi access point designated by the device user, the overall device risk scenario is high and the device may be accessible to a large number of potential network based attack vectors. Unrestricted WiFi access is not recommended on any agency owned device, but must be assumed to exist on any personally owned device authorized to access CJI. Significant compensating controls may be needed to ensure devices accessing CJI over ‘public’ WiFi access points are not susceptible to communications network eavesdropping, credential hijacking or any of the various potential man-in-the-middle attacks possible through access point spoofing. The communications security risks can be significantly mitigated by mandatory device configurations (e.g. MDM based policy) that only allow devices to connect to cryptographically verified agency controlled WiFi access points.

WiFi only or devices with ‘on-demand’ cellular access (e.g. user or event driven cellular access initiated from the device and not from a centralized management location) are significantly more at risk from data loss subsequent to device loss or theft as there is no guarantee the tracking or remote wipe can be initiated once the device is out of agency control. This can be mitigated by utilizing tracking/anti-theft products that require a periodic network connection to authorize access and perform automated device locking (‘bricking’) or remote wipe if network connections are not made within a specified period. Software of this nature is generally available for full-featured laptops but may not be available for limited-feature mobile operating systems.

Cellular (always on) + WiFi Network

This is a hybrid scenario that has become typical with most ‘smartphones’. These devices contain both the always on cellular connection, but may also be configured to access local WiFi networks for enhanced bandwidth. In considering devices with these technical characteristics, the theft/loss risks are similar to the cellular only scenario (due to tracking and remote access through the cellular connection), while the data and network based risks must be considered to be similar to the WiFi scenario unless the capability of the device to connect to WiFi networks is limited by technology or policy to agency owned WiFi Access Points configured in accordance with the CJIS Security Policy. Careful consideration must be made to the particular configurations, management systems, and human oriented operational policies based on the particular technical capabilities and configurations of these types of devices.

Incident Handling (CJIS Security Policy Section 5.3)

Additional or enhanced incident reporting and handling procedures will need to be developed to cover mobile device operating scenarios. Various exploits and methods to compromise mobile devices require either specialized equipment or lengthy operations to implement. Rapid response to mobile device related incidents can significantly mitigate the risks associated with illicit data access either on the device itself or within online data resources associated with the device through an application or specialized interface. However, parallel or special incident handling procedures with associated equipment or systems may need to be put in place to properly respond to incidents involving mobile devices. This section lists three areas where enhanced incident handling and

response processes may need to be implemented to ensure mobile device compliance to the incident handling policy in Section 5.3.

If personally owned devices are utilized within the environment in a Bring Your Own device (BYOD) scenario, specialized and costly incident handling procedures and processes may need to be developed to support compliance for those devices. The costs associated with enhanced incident handling procedures may need to be incorporated in the cost and risk based analysis to allow personally owned devices in the BYOD scenario, as the technical methods and risk to achieve compliance under BYOD scenarios may exceed any cost savings potentially achieved through BYOD.

Loss of device Control

Mobile device users should be trained and provided with explicit user actions in case positive control of a mobile device is lost for any period of time. Loss of positive control means the device is in the physical control of non-CJIS authorized individual or the device is left unattended in an unsecure location (e.g. counter of the coffee shop). Even if the device is recovered quickly there is significant risk that either the device settings could be tampered with or data on the device could be illicitly accessed. The level of detail and particular scenarios identified in the agency incident response plan should be consistent with the presence of persistent CJI on the device or the technical means used to access CJI from the device (e.g. ask the question: “Is it reasonable to assume CJI could be accessed”) as well as the degree of device configuration control exercised by the user from the device main login. At a minimum, special incident handling procedures should be developed for the following scenarios:

- Device known to be locked, control loss of minimal duration
- Device lock state unknown at time of control loss, duration of loss minimal
- Device lock state unknown at time of control loss, duration of loss extended
- Device known to be unlocked at time of control loss, duration of loss more than momentary.

NOTE: Organizations should define appropriate time value criteria based on the operational environment for the above scenarios. For instance, a ‘momentary’ loss of control might be considered a matter of seconds in a situation where no one could reasonably have accessed the device, while ‘minimal’ durations might include a few minutes of time and ‘extended’ periods would be any time longer than a few minutes.

Other scenarios should be addressed as appropriate to the intended device employment, with explicit user and organizational actions identified based on the device technologies and any organizational management capabilities.

Total Loss of device

Incident response scenarios for the total loss of the device should be developed based on the methods/storage of CJI on the device, the lock state of the device at time of loss (known locked, known unlocked, or unknown), and the technical methods available for remote tracking or wiping of the device. It is critical to implement incident handling procedures quickly in this case. Remote wipe functions can be implemented for always on cellular devices with a high potential for success that may include positive confirmation from the device that the wipe was completed. However, for WiFi only and on demand cellular devices, incident handling procedures that lock the device out

of accessing CJI may be necessary, while there would be no guarantee that any CJI stored on the device could not eventually be accessed. For this reason, CJI should not generally be stored directly on WiFi only or on-demand cellular devices unless an extremely robust anti-tamper system is in place on the device itself.

Potential device Compromise (software/application)

Incident response scenarios for potential device compromise through intentional or unintentional user action should be developed to ensure compliance with policy. This includes rooting, jailbreaking or malicious application installation on the device during a loss of device control scenario or inappropriate user action in the installation of applications to the device (compromise can occur from either intentional threat agent actions or accidental user actions). Triggers for this incident handling process may be driven from either user notification or electronic detection of device tampering from an audit or MDM compliance check.

Audit and Accountability (CJIS Security Policy Section 5.4)

The ability to implement some Audit and Accountability functions specified in the CJIS Security Policy on mobile devices with limited function operating systems (e.g. Android, Apple iOS) is not natively included within the operating system. Either additional device management systems, enterprise mobility management (EMM) or MDM, or auditing from systems accessed by the mobile device will be necessary to ensure appropriate levels of auditing exist.

Auditable Events (reference 5.4.1)

Some of the specific audit requirements in the CJIS Security Policy may not be technically relevant to the mobile operating system due to its internal functioning. To achieve compliance with the CJIS Security Policy it will be necessary in most cases to utilize some form of MDM or EMM system. Additional auditable events that compensate for the technical limitations of limited function mobile operating systems may be available through the use of MDM systems (e.g. association of event with global positioning system (GPS) location of the device). Specific auditable events of interest in the mobile environment will depend on the intended device usage, compartmentalization of data on the device, and options available with the specific technologies employed. For instance, item 2 in Section 5.4.1.1 indicates an auditable event includes attempts to modify elements of user account modification. Due to the limited internal functions of mobile operating systems, this event type is not relevant to the operating system itself as they are generally provisioned with only a single non-modifiable user account on the device. To achieve compliance in a scenario where CJI is stored or accessed from a secure application on the device, auditing of access to the secure application either through application design, or third party MDM capability may provide an acceptable compensating control. For compliance with the policy each auditable event and event content must be compared to the particular technologies and applications employed to determine if adequate compensating controls are being met for audit items that either do not apply to mobile technologies or cannot be implemented within the technology itself.

Alternative and compensating controls that provide detailed audit of access to CJI either on the mobile device itself or through a controlled application to a central server may provide equivalent auditing capability to the events specified in the policy. However, multiple auditing systems may be required to replicate the auditing provided at the operating system level by a full function operating system. Therefore, the overall auditing design should take into account retrieval and

consolidation of events or audit data from multiple auditing systems as appropriate to comply with policy.

Audit Event Collection

Mobile devices without an ‘always-on’ cellular connection may pose technical challenges to ensure any audit records collected and stored on the mobile device itself can be retrieved for review and analysis per the CJIS Security Policy. Alternatively systems which explicitly require a network connection to a central server to access data or decrypt on-device storage may provide acceptable audit event collection and reporting since there is a guarantee that network connections must be in place for CJI to be accessed. Careful consideration should be made regarding the accessibility of audit records when developing the mobile audit scheme.

Access Control (CJIS Policy Section 5.5)

Access control associated to limited functionality mobile operating systems will typically operate in a different manner than full function operating systems. For instance there is normally not a provision for multiple user accounts on many mobile operating systems which may mean the policy requirements for access control (e.g. regarding account management) would not be apply to the mobile operating system, but should rather be applied to a particular application, either stand-alone to the device or as part of a client server architecture. Application of access control policy identified in the CJIS Security Policy will often need to be applied to elements of the total system beyond the device operating system.

For example, CJI stored or accessed from a secure mobile application that requires connectivity to a CJIS authorized server architecture could potentially accomplish most or all of the access control policy elements based on user authorization via the secured application and be largely independent of the mobile operating system. Alternatively, if storing CJI in ‘general’ purpose data storage containers on a mobile device it may not be possible to achieve compliance with the CJIS Security Policy. Careful consideration and deliberate design of mobile applications or data storage will be required to achieve compliance on mobile devices.

Due to the inherent nature of limited function mobile operating systems, very tight access controls to specific data is actually implemented within the operating system. This effectively prevents applications from accessing or manipulating data associated with other applications to a very high degree of confidence as long as the device is not rooted or jailbroken. However, the device user is automatically granted access to all device data through the associated application unless the application itself has a secondary authentication and access control methodology. Additionally, since basic device functions (e.g. phone) are typically protected using the same password or PIN as the device level encryption, use of a weak PIN to allow easy access to basic device functions largely negates the value of the integrated device encryption.

If personally owned devices are utilized within the environment (BYOD scenario), specialized and costly access control methods may be required to reach compliance with CJIS Security Policy. The costs associated with enhanced access control procedures and technologies should be incorporated in the cost and risk based analysis to determine whether or not to allow personally BYOD, as the technical methods and compensating controls required for CJIS Security Policy compliance are likely to exceed any potential cost savings for implementing BYOD.

Device Control levels and access.

Limited function mobile operating systems are typically very constrained on the levels of access provided to the user. However, intentional user actions (e.g. installing an application and accepting inappropriate security access levels for that application) may bypass some of the built in security protections inherent in the limited functionality devices. Compliance with CJIS Security Policy may be difficult without the addition of strict device control policy. In a mixed environment (e.g. agency owned devices and BYOD), access control policy with BYOD systems may be impractical or impossible to fully implement.

Embedded passwords/login tied to device PIN.

Limited function mobile operating systems typically allow the association of multiple passwords and access credentials with particular applications. The system access provided by these embedded credentials will often be tied to the device password or PIN. An example would be access to device integrated email and calendar applications. Alternatively a 'corporate' email application may independently encrypt the data associated with the application and require a separate login from the device itself. Access to CJI utilizing only the device level password or PIN and device embedded credentials is not compliant with CJIS Security Policy unless protected with Advanced Authentication, which is not currently possible on most devices. Therefore, use of integrated device functions (e.g. built in email or chat) to store or transmit CJI would also not be compliant.

Access requirement specification

In general, due to weaknesses associated with password guessing based on analysis of fingerprints or swipes on the device touch screen, short (4-8 digit) device PIN numbers provide limited security to a determined password guessing attack. Conversely, utilization of a robust password at the device level may be inconsistent with quick access to basic device functions (e.g. phone). When developing specific CJIS compliant access control and authentication schemas a layered approach with the device PIN protecting only the basic device functions (e.g. phone, camera, non-secure applications) and a more robust password or multifactor authentication used to protect applications or data storage may achieve policy compliance where the device password/PIN would not. In a layered security deployment, careful attention must be placed on the capability to share data (e.g. cut and paste or screenshot functions) between secure applications with CJI or CJI access and basic device functions with limited security controls.

Special Login attempt limit

Depending on the access and authentication scheme applied to the mobile device, it may be appropriate to fully comply with the CJIS login attempt limits within a secure application or container and not solely at the device level. However, the device itself should have login attempt limits consistent with the risk associated to the data or configurations accessible on the device itself. Since mobile devices are inherently portable, and can easily be removed from a location. Brute force attempts to gain access to the system, especially when protected only by a short PIN, are likely to be successful given sufficient time. Special consideration should be made based on device connectivity methods (cellular, WiFi, etc) on the appropriate number of unsuccessful login attempts that will be allowed and the resultant actions taken by the device. Most devices either natively allow for the device to wipe itself after a failed number of attempts, or allow the application of EMM/MDM applications to perform wiping actions after a predetermined number of failed login attempts.

Login failure actions

Mobile devices with or without MDM software can typically be configured to perform actions based on serial unsuccessful login attempts. Appropriate actions to configure may be dependent on the data resident on the device and the connectivity method employed by the device. Most devices can be configured to delete all data on the device and/or issue an alert to the network if a number of incorrect passwords are entered. This is a very advantageous feature, however specific configuration of the number of attempts and resultant action must be considered against the state of the device after an unsuccessful attempt action is triggered. A full device wipe will typically leave the device in a fully or partially non-functional state which could introduce risk if part of the intended use is time critical phone calls. Where possible, full device wipe associated with unsuccessful attempts at the device level password should be configured but the number of invalid attempts may exceed the CJIS Security Policy at the device level if all CJI on the device is protected by an additional layer of encryption protected by a subsequent secure application authentication method that is technically prevented (via complexity rules or entry rules) from being the same as the device level authentication and the secure application is configured in accordance with the policy and also contains a secure data wipe capability after a specified number of incorrect authentication attempts.

System use Notification (CJIS Policy reference 5.5.4)

Agency policy should include specific mandatory language consistent with the CJIS Security Policy to identify the device restrictions and consent. However, due to screen size limits, some mobile devices may not be technically capable of displaying the full text used with traditional operating systems. To achieve compliance agencies should contact their legal department for appropriate wording of a short version of the system use notification that can be set to display within the constraints of the device lock screen. This may be accomplished through embedding the text into an image displayed on the lock screen or some other external device labeling method if the device does not permit sufficient text to be displayed.

In a BYOD environment or mixed (agency owned and BYOD), it may be necessary to develop or deploy custom applications that can achieve compliance with the system use notification upon access and prior to any CJI access being allowed.

Session Lock (CJIS Policy reference 5.5.5)

Due to the portable nature of mobile devices the session lock limit in the general CJIS Security Policy may be excessive in the mobile environment for certain device functions and insufficient for other functions based on intended device usage. Agencies should examine the minimum lock time practical for all mobile devices based on their employment scenario and ease for which a user can manually lock the device. The actual session lock times should be adjusted as appropriate to the device type, device operational location, and the data accessible on the device when unlocked. Pocket size devices are at greatest risk if screen lock times are insufficient, however, for devices used in emergency response or communication, extended lock times at the basic device level may be considered if CJI is subsequently protected by an application or web interface utilizing more stringent secure locking functions. A well designed solution may include multiple session lock settings at the device and individual application levels to ensure the CJIS Security Policy requirements are met for CJI access, while other device functions are accessible under different session lock configurations.

Device WiFi Policy

Specific WiFi configuration policy should be developed based on the intended use environment and data access requirements for the device. The policy should explicitly cover configuration of device connections. Technical methods specific to the mobile technologies may need to be implemented to ensure all mobile devices are compliant with CJIS Security Policy. Current CJIS Security Policy provides detailed configuration requirements for WiFi connections, however it was originally intended for defining requirements for fixed infrastructure WiFi (802.11) supporting wireless within a facility. The security requirements identified for fixed infrastructure installations are applicable to mobile usage, however there are several mobile specific scenarios where the requirements may not be clear. The following sections identify areas not specifically covered in the existing policy that will require special handling to ensure wireless connections are compliant.

Hotspot capability

Many mobile devices now include the capability to activate an internal WiFi hotspot that allows other devices to connect through the hosting device to the internet over the devices cellular radio. While this is a potentially valuable capability when multiple law enforcement devices may need localized internet or network access, mobile hotspots should be configured as consistent with the CJIS Security Policy on wireless access points. Connections must only be accepted from known and approved devices in order to protect the integrity of the hosting device as well as the communications security of other connected devices. Since most mobile hotspots are not technically capable of providing the device authentication required for infrastructure wireless, use of mobile hotspot capability should assume the overall portable WiFi network itself is not secure and CJI should not be transmitted or exposed on the network without appropriate encryption.

Connection to public hotspots

There are significant risks to connecting to public wireless access points. Rogue access points masquerading as legitimate public access points may allow for man-in-the-middle, eavesdropping, and session hijacking attacks. While not specifically prohibited in the current CJIS Security Policy, it is recommended that connection to public internet access points be technically restricted by device configuration or MDM systems if possible. CJI access mechanisms from mobile devices should include robust authentication methods specifically designed to prevent interception or hijacking of CJI or user information through the use of a rogue access point masquerading as a legitimate public wireless access point. Transmission encryption alone may not provide sufficient protections when device connections originate at public hotspots. Since the public hotspot controls access to all network services at the connection point (e.g. Domain Name System) attacks against the transmission path are possible that would not normally be feasible in a fixed environment where communications exist between two secured network enclaves.

Cellular Service abroad

If mobile devices are used outside of the United States, especially if connected to foreign cellular networks, specific handling procedures may need to be developed for the use of the device while abroad and the assessment or configuration check of the device state once the devices are returned to the United States. Certain device internal functions on cellular devices may be modified or compromised by the cellular carrier as the devices are intended to have certain parameters configured by the cellular service provider which is considered a 'trusted' entity by the device.

Cellular carriers within the United States are constrained by United States laws regarding acceptable modifications to devices. Similar legal constraints cannot be assumed to exist in some areas of the world where laws and regulations for data and personal privacy may allow cellular carriers significantly more leeway in changes made to devices on their networks.

Security plans involving cellular connected devices that will be connected to foreign cellular networks should include technical and policy controls to ensure device use while abroad, data resident on the device while abroad, and the software integrity of the device once returned to the United States are all appropriate to the specific device and threat levels associated with the expected foreign travel. This should explicitly include considerations for devices in which an internal subscriber identity module (SIM) card is inserted into the device to obtain Global System for Mobile (GSM) cellular connections abroad to ensure any residual data on the SIM card is properly purged. Additionally, incident handling procedures may need to specify more stringent responses to even momentary loss of device control, and it may not be possible to assume tracking, anti-theft, and remote data wipe functions that work in the United States would be functional in all potentially visited geographic and political regions.

Bluetooth

Mobile devices utilizing Bluetooth should be evaluated for their ability to comply with the CJIS Security Policy Bluetooth requirements prior to acquisition. This includes the data device itself and any authorized Bluetooth accessories which will be associated to the device. While the technical security in current versions of Bluetooth is significantly stronger than legacy versions, mis-configuration of devices can still pose a significant threat in the mobile environment. If not specifically utilized for a required purpose, it would likely be most cost effective to disable or restrict the device Bluetooth radio utilizing device configurations or an MDM product. Additionally, the using agency may need to develop technically extensive training or user awareness programs to ensure use of Bluetooth capability does not render the device out of compliance if device users have the ability to make Bluetooth associations to the device. Specific instructions or guidance for specific devices could be developed to ensure all implementations are compliant.

Voice/Voice over IP (VoIP)

Cellular voice transmissions are distinctly different at the technical level than Voice over IP (VoIP) transmissions using voice/video applications (e.g. FaceTime, Skype). The use of VoIP is not specifically granted the exemption identified in CJIS Security Policy Section 5.5.7.3.2. Agencies wishing to use capability of this type should ensure the specific technical implementation complies with the Policy on authentication and data encryption.

Chat/Text

Device integrated chat/texting applications and many common third party chat applications authenticate and are identified using embedded passwords or the device identifier only. These functions should not be considered secure or appropriate for transmission of CJI data. Texting functions that utilize a cellular service providers Short Message Service (SMS) or Multimedia Messaging Services (MMS) functions do not constitute a secure transmission medium. Third party applications utilizing appropriate encryption and authentication methods independent of the device password/PIN may provide a compliant solution where the device integrated utilities are will not provide a compliant solution.

Administrative Access

Local administrative access to the mobile device, regardless of device category should be restricted by some mechanism. For traditional operating systems, configuration of a separate administrative account other than that used for normal logins to the device is an acceptable method to ensure appropriate access permissions to the mobile user for which they are authorized. However for limited functionality mobile operating systems (e.g. Android, Apple iOS) internal permissions and accounts assume a single authorized device user with explicitly defined permissions. Those permissions may be modified through policy applied to the device, but are typically global to the device itself. As a result, to ensure appropriate separation of access permissions, it may be required to ensure specific applications or software on the device are configured with individual authentication methods to separate application data from ‘general user’ access. Without additional authentication at the application level, access to specific application data would be available to any user with the ability to unlock the device. This may be appropriate in some scenarios with a high degree of assurance that the device can only be accessed by a single user, but sufficiently stringent device passwords and short screen lock times may prove problematic for practical use of some device functions. An alternate method to ensure strict separation of ‘routine’ device functions which may be accessed by multiple individuals (e.g. phone function if loaned to someone for a critical call) is to ensure any method used to access or store CJI has a separate and more stringent authentication method configured with rules that make it impossible to use the same authentication credential (e.g. PIN/Password) on both the device authentication and the application or function with access to CJI.

Rooting/Jailbreaking

‘Rooting’ (Android OS) or ‘Jailbreaking’ (Apple iOS) refer to intentional modifications to the mobile device operating system in order to grant the device user or an installed application elevated control that would not normally exist on the device. The security model internal to the various mobile device architectures vary significantly, however the common effect of rooting or jailbreaking the devices is to bypass many or all of the built in security features. The security feature bypass may be universal to all device features and installed applications once completed. Intentionally rooting or jailbreaking mobile devices should be avoided in any scenario as it potentially defeats all built-in data access and segregation controls on the device. Additionally the rooting or jailbreaking process itself has a heightened risk of introducing malicious code as part of the process, and also substantially increases the risk for malware to infect the device through user action. Extreme caution should be used if software is being installed that requires the devices to be rooted or jailbroken for the software or application to function. This is inclusive of purported security software that requires a rooted or jailbroken device to function. For example, on both the Android and Apple iOS platforms, the built-in security features for data access and memory segmentation prevent the effective operation of ‘traditional’ anti-virus and intrusion detection/prevention software. Software or applications purporting to perform these functions but requiring rooting or jailbreaking of the device and may actually accomplish the anti-virus or IDS/IPS function but are also likely to significantly increase the overall risk associated to the device by effectively disabling most or all of the integrated security features. A careful risk-based assessment should be conducted by a trained security professional prior to allowing the operation of any rooted or jailbroken mobile devices regardless of intended use. Significant compensating controls would be required to return a rooted or jailbroken device to minimal compliance with most of the CJIS Security Policy and would likely not be a cost effective approach.

NOTE: There is a distinction between rooting a ‘stock’ Android installation vice the installation of a separately supported secure operating system. There are secure versions of Android available or that can be developed based on the open source Android source code and compiled for installation on a particular hardware device. Installation of a secure, supported mobile operating system that replaces the device original operating system may significantly enhance the security of the device and should not be confused with ‘rooting’ and Android installation. Due to the close integration of operating system security with hardware elements, and the proprietary nature of Apple source code, there are not currently separate ‘secure’ versions of the Apple iOS and it is unlikely they will be developed.

Identity and Authentication

Due to the technical methods used for identity and authentication on many limited functionality mobile operating systems, achieving compliance to CJIS Security Policy may require layering of identification and authentication mechanisms. With the complexity and large number of potential identity and authentication solutions in the mobile environment emphasis must be placed on designing secure identity management and authentication architecture prior to the selection of individual devices or applications. Failure to consider a robust identity and authentication scheme as part of system design or acquisition will significantly increase the risk of subsequent noncompliance with CJIS Security Policy and potential added costs for a remedial solution. Many identity and authentication schemes used by existing commercial applications may make claims that appear to be consistent with CJIS Security Policy Advanced Authentication requirements, however, extreme care must be taken to ensure the actual technical implementation is compliant with policy.

Utilizing Unique device Identification

Some commercial applications and features integrated with some mobile operating systems permit the mobile device to be uniquely identified in a cryptographically robust manner. Any authentication schema that considers the possession of the mobile device as a factor in uniquely identifying and authenticating a CJIS authorized user must also include factors beyond than mere possession of the device. Larger form factor devices that cannot be carried on the person of the authorized user should not rely on possession of the device as an identifying factor, but may still include identifying capability within the device to provide assurance that the device itself is an authorized device. This should still be coupled with multi-factor advanced authentication to the device itself or the application hosting CJI. Coupling unique device authentication with robust advanced authentication of the user provides a high degree of confidence that both the specific device and the operator of the device are correctly identified. Utilizing device unique identification in order to authorize initial connections from the remote device back to the CJI hosting system or enclave provides additional protection to the CJI hosting system to reduce the attack surface of the hosting system and should be considered a good practice, but not in itself an authentication mechanism for the device user.

Certificate Use

One method for uniquely identifying mobile devices is to place part of a public key pair on the device in the form of a public key certificate. While there is value to ensuring the device itself can authenticate to a system supplying CJI, and may provide a critical layer of identification or authentication in a larger scheme, a certificate alone placed on the device should not be considered valid proof that the device is being operated by an authorized CJIS user, only that the device itself is authorized to host CJIS users. Additional user identification and authentication should be used to supplement any device certificate installed. Using a PIN or password separate from the device login to ‘unlock’ the certificate from cryptographic storage within a secure application will provide an additional layer of security and may increase the confidence level the device is being used by the intended user. However, use of public/private key pairs or pre-shared encryption keys can be utilized as part of an architecture to protect against certain session hijacking or man-in-the-middle attacks a mobile device may be susceptible to if connected to public internet connections.

Certificate Protections

Any certificates or cryptographic keys stored on any mobile device should include protections against the certificate or key being extracted from the device. Additionally certificates or other keys stored on mobile devices that grant the device special access or unique identification should be configured for remote wipe on demand or self-deletion based on a number of unsuccessful login or access attempts. Alternatively, methods may be used to revoke or invalidate the unique certificate or keys associated with a device.

Minimum Password/Pin (Reference CJIS Security Policy Section 5.6.2.1)

The minimum password protections identified in the CJIS Security Policy may not be appropriate for the device PIN/password due to immediate access requirement for some device functions (e.g. phone function) secured by the device PIN/password and the difficulty to enter a complex password under emergency conditions on a small screen. In cases where the risk of a complex password on the device itself is deemed significant, a layered authentication approach may be necessary where CJI or access to CJI is protected via one or more additional layers of access control beyond the device PIN/password. In cases where the CJI or access to the CJI is cryptographically segregated from applications accessible using the device level PIN/Password (e.g. secure application or secure browser vice the built-in browser) the authentication mechanism for the secure application or browser may satisfy the CJIS Security Policy requirements if fully compliant as a stand-alone application.

Configuration Management

Due to the potential for inconsistent network access or monitoring capability on mobile devices, methods used to monitor and manage the configuration of traditional full-featured operating systems may not function properly on limited function mobile operating systems. Configuration Management systems in the mobile environment may be designed in order to duplicate some of the functions typically performed by traditional anti-malware systems that will not function properly on some mobile operating systems.

Mobile Device Management (MDM)/Enterprise Mobility Management (EMM)

MDM and EMM systems and applications coupled with device specific technical policy can provide a robust method for device configuration management if properly implemented. MDM capabilities include the application of mandatory policy settings on the device, detection of

unauthorized configurations or software/applications, detection of rooting/jailbreaking of the device, and many other security policy related functions. In many cases, the most cost effective way to achieve CJIS Security Policy compliance on mobile devices is the selection of MDM or EMM applications and infrastructure appropriate to the mobile operating systems and intended access to CJI on the mobile devices. MDM/EMM functions may be applicable to most of the CJIS Security Policy requirements and allow for significant compensating controls in areas where traditional methods of CJIS Security Policy compliance are not technically feasible. Section 5.5.7.3.3 of the CJIS Security Policy specifies the minimum functions required for MDM. However, careful selection of the MDM product will potentially provide a cost effective method for additional areas of compliance in the access, auditing, incident response, authentication, media protection and system integrity sections of the CJIS Security Policy.

Device Backups/Images

Device images and backups provide protection against data loss, but also provide a method to quickly recover a device after damage or potential compromise. Due to an inherently limited ability to access the internal file structure of mobile devices, it can be difficult to easily identify a device compromise or illicit modification of the device. Some device imaging and assessment software may provide a secondary forensic capability, especially if there is intent for the device to be used outside the United States.

Bring Your Own device (BYOD) employment

BYOD environments pose significant challenges to the management of secure device configurations. In many cases it may be impossible to apply effective security that is acceptable to the device owner or it may require extremely costly compensating controls to allow access to CJI on personally owned devices. While allowed by the CJIS Security Policy, agencies are advised to conduct a detailed cost analysis of the ancillary costs of compliance with CJIS Security Policy on personally owned devices when they are approved for use. In some cases, a BYOD user may agree to abide by the same device configurations and limitations as imposed on an agency owned device, but signed user agreements should still be in place to ensure the agency has a legal right to recover or clear the device of all data prior to device disposal or employee termination. In other cases, robust secure applications may provide acceptable levels of compliance in a BYOD environment for limited CJI access but application design and architecture should assume the device itself is un-trusted. If MDM/EMM software capable of detecting rooting or jailbreaking of the device is not installed, any CJIS or data access occurring from the device is at a substantially higher risk of compromise.

Configurations and tests

Common configurations specific to all employed mobile devices should be developed to ensure compliance. Configuration tests should be developed and executed on all versions of mobile devices under all possible connectivity scenarios to ensure CJIS Security Policy compliance under all expected operating conditions. Since mobile devices can expect to operate in different physical and network environments, testing and validating correct security functions is more critical than on fixed computing platforms. Additionally, security functions that function properly on one version of a mobile operating system on a particular device may not function in the same manner even on the same version on a different device or a different version on the same device.

Media Protection

Some mobile device hardware platforms include the ability to add removable storage in the form of memory cards. This function is primarily related to Android and Windows mobile platforms and is intentionally limited on Apple devices, but may be possible through certain application functions. While the Android platform performs robust cryptographic separation of data stores between applications within the ‘internal’ storage of the device, the Android OS does not provide secure separation of data stores on ‘external’ storage. Some Android hardware devices include additional storage hardwired inside the device that is classified by the operating system as external storage and the normal separation between applications accessing that storage is not applied. Each potential device considered for acquisition must be assessed regarding specific ‘external’ media protection requirements which may actually include built-in media or storage.

Protection of device connected media

As a result of the limited protection and encryption capabilities applied to device removable media and SIM cards for cellular provisioning that include onboard data storage, all externally removable media or memory should be handled consistently with the CJIS Security Policy on media protection.

Encryption for device media

While most mobile operating systems have the capability to encrypt internal storage, it may require specific device settings to be enabled. All mobile device storage should meet the encryption requirements identified for media in the CJIS Security Policy. Specific settings may need to be applied to ensure proper encryption is actually employed. Additionally, the device built-in encryption capability is typically tied to the device PIN or password. Depending on the device PIN or password requirements the integrated encryption may be easily bypassed by password guessing and appropriate consideration should be made to ensure additional encryption protected by advanced authentication methods be applied to all CJI.

Physical Protection

Due to small form factors and the fact that mobile devices are often stored in lower security areas and vehicles, physical protection of the devices must be considered in both policy and training. Physical protections will often be the responsibility of the assigned device user and physical protections typically inherited by individual information systems from a secure facility will not be available to mobile devices which will require compensating controls to achieve compliance.

Device Tracking/Recovery

MDM software as well as some integrated mobile operating system functions may allow tracking of stolen or lost devices via ‘always-on’ cellular data connections and the devices built-in GPS. Device tracking with WiFi only or ‘on-demand’ cellular access may not be reliable. Enabling device tracking capabilities, while not a replacement for secure storage, could be a compensating control used to substantially reduce overall device risk in some scenarios. Device tracking is not currently required in the CJIS Security Policy but should be applied to agency owned devices where possible as a risk mitigation factor. Enabling of device tracking on personally owned devices in a BYOD environment may raise employee privacy concerns and should be considered only for critical systems with the full knowledge of the employee and concurrence of the legal department. This is an enhanced risk that must be accepted for BYOD employments and should be considered

when allowing BYOD employment. Device tracking is available for both limited function mobile operating systems as well as traditional operating systems installed on laptop devices.

Access to device tracking software or applications within the organization should be controlled with limits and formal processes required to initiate a tracking action. It is advisable to include appropriate clauses in user agreements under what conditions and controls the organization applies to device tracking.

Devices utilizing unique device identification/certificates

Devices utilizing unique device identification or have installed certificates may require additional physical protection and/or additional incident handling steps in case of device loss in order to ensure the device unique identifier or certificate is immediately revoked or disabled. Additional physical protection rules or policy would be appropriate for any device which contains access mechanisms tied to the device.

System Integrity (CJIS Policy Section 5.10)

Managing system integrity on limited function mobile operating systems may require methods and technologies significantly different from traditional full-feature operating systems. In many cases the requirements of Section 5.10 of the CJIS Security Policy cannot be met with a mobile device without the installation of a third party MDM or EMM application and supporting server infrastructure.

Patching/Updates

MDM software may provide compliance to the Section 5.10.4.1 patch management requirements for particular platforms and software versions. However, devices without ‘always-on’ cellular connections may not be reachable for extended periods of time by the MDM or EMM solution either to report status or initiate patching. Supplementary or manual device accountability methods may need to be implemented to account for devices without persistent connections to ensure their patch and update state is current. Alternatively, some patches or system updates may not be practical over cellular connections and will require connection of devices to a WiFi network. Compliance with CJIS Security Policy requirements through purely technical means may not be practical and considerations should be made for aggressive management of devices through training and mandatory periodic connection of devices to organizationally managed WiFi networks.

TECHNOLOGY NOTE: Apple and Android based devices have different potential issues regarding device operating system updates. Apple maintains support for updating the operating system on Apple hardware for several device generations (typically 3-5 years) and provides a robust mechanism for system updates. However, updates to Android based systems are driven by the individual device manufacturer which may or may not support regular updates to current Android operating system versions. Additionally, different Android device vendors may offer updates/upgrades to the Android operating system on different schedules, which can complicate environments utilizing Android devices from multiple manufacturers.

Malicious code protection/Restriction of installed applications and application permissions

MDM or EMM software will typically allow restrictions on installed applications. One of the few effective attack vectors to compromise mobile operating systems is to manipulate the device user to install a malicious application. Even though the application may be restricted from accessing

other application data, it may have some access to common data stores on the device and access to device functions (e.g. GPS, microphone, and camera) that are undesirable. Unrestricted installation of applications by the device user could pose a significant risk to the device.

Malicious code protection using traditional virus scanning software is technically infeasible on most limited function mobile operating systems that are not rooted or jailbroken. The integrated data and program separations prevent any third party installed program from accessing or 'scanning' within another application data container. Even if feasible, power and storage limitations would be prohibitive in the effect on device battery life and storage capacity on most mobile devices. However, the cryptographic separation between applications and effective application virtualization technologies built into common mobile operating systems partially compensate for the lack of traditional virus scanning technologies. Appropriately configured MDM software is capable of checking the installed applications on the device and reporting the software inventory to a central management console in a matter analogous to traditional virus scan detection of unauthorized software. This behavior is analogous to the software inventory performed by anti-virus products and can provide a high degree of confidence that only known software or applications are installed on the device. While it is theoretically possible to bypass the application sandboxing and data segregation protections to compromise a mobile device through the web browser, the attack methods required are significantly more advanced than those required for a traditional full-featured operating system. Malicious code protections on the device web browser can be enforced through the use of a properly protected web proxy which the device is configured to use as a mandatory device policy. The most common method of malicious code installation is enticing the user to manually install the malicious app which can be mitigated on organizational devices using an MDM or other application installation restrictions which prevent the user from installing unauthorized or unknown applications. Mitigation of this issue within BYOD environments may not be possible and will present a significantly enhanced risk to the device.

TECHNOLOGY NOTE: In the particular area of application installation there is a significant difference between the behavior of Apple iOS and Android platforms. Apple cryptographically restricts the way applications will execute on the device and assigns mandatory application permissions when the application code is signed prior to release on the Apple App Store for distribution. Apps on the Apple platform must conform to Apple's policy on app behavior and cannot exceed their design permissions on access to common device functions once the app has been signed and distributed. However, the Apple method does not typically advertise the precise internal permissions granted to the app to the user prior to installation. At runtime, the app is required to request user permission to access certain device functions, and the user may agree or not agree, which may introduce risk if they are unaware of what they are agreeing to allow. Unsigned or un-trusted apps are cryptographically prevented from executing on non-jailbroken iOS devices. Apple provides a mechanism for organizations to distribute custom apps within an organization with equivalent protections but all receiving devices must have a special certificate installed that will only allow official App Store and the organization custom apps to execute.

Conversely, the Android platform, while also requiring app code signing, allows for self-signed code which can be distributed by means other than an official app store and execute on any Android device. Application permissions are presented to the user once at app installation but ramifications of agreement to certain app permissions may not be obvious to a non-technical user. Permissions in the Android model require user acceptance of all app requested permissions or the app is denied

installation, which can result in unwise user acceptance of excessive permissions in order to gain functionality provided by the app.

On either platform user installation of applications can significantly change the security state of the device. Applications may be able to transmit and receive data or share device common data with other devices over the network or local WiFi or Bluetooth connection. On either platform it is highly desirable to limit allowable applications to a pre-approved pool of apps via MDM or organizational App store structures and device policy. However, the risks associated with uncontrolled app installation is several orders of magnitude greater on Android based devices.

WARNING: Rooted or jailbroken devices are modified in such a manner that the built in protections against malicious code are effectively disabled. A rooted or jailbroken device would require significant and costly compensating controls to achieve compliance.

Firewall/IDS capability

Traditional device or “personal” firewalls as identified in CJIS Security Policy Section 5.10.4.4 may not be practical on limited function mobile device operating systems but significant compensating controls are available. By default, mobile device operating systems have a limited number of system services installed and carefully controlled network access. To a certain extent the mobile operating system performs similar effective functions as a personal firewall would perform on a general purpose operating system. Potential compensating controls for the five (5) personal firewall requirements specified in Section 5.10.4.4 are listed below:

1. Manage Program Access to the Internet: On agency controlled devices with an MDM, limiting the apps installed on the device will effectively perform the same function. Since no software or apps can be installed without MDM approval a robust approval process can effectively ensure internet access is only granted to approved apps. Built-in apps and functions can also be limited on network access by the MDM.
2. Block unsolicited requests to connect to the user device: Default configurations for mobile operating system platforms typically block incoming requests. It is possible to install an app that may ‘listen’ on the network and accept connections, but the same compensating control identified in item 1 will mitigate the likelihood of that occurring.
3. Filter incoming traffic by IP address or protocol: Protocol filtering effectively occurs due to the limited function of the operating system as long as no installed application opens network access ports. The mitigations in 1 effectively compensate for this control as well.
4. Filter incoming traffic by destination ports: Same as 3.
5. Maintain an IP traffic log: This may not be technically feasible on most mobile operating system platforms as maintaining this log would require access to lower level operating system functions that are not accessible unless the device is rooted or jailbroken. However, individual Apps that communicate over the network or accept connections from the network may permit logs of IP traffic associated to that application to be stored.

Spam Protection

Spam guards installed on corporate or organizational email systems may effectively accomplish the spam protection requirements for the CJIS Security Policy on mobile devices if properly configured to block spam before delivery to the device. If no upstream spam guard is installed on the mail server the mobile devices accesses, the device may not have adequate spam protection. Additionally access to internet based email (web mail) would need to be restricted to web mail with appropriate spam and/or antivirus protections to ensure compliance.

Periodic system integrity checks

One method to compensate for the technical infeasibility of traditional anti-virus and malicious code protection is to install an MDM that performs periodic system integrity checks that validate device configuration and status against an approved baseline. Deviations may provide indicators of potential device compromise or mis-configuration.

G.5 Administrator Accounts for Least Privilege and Separation of Duties

Administrator Accounts for Least Privilege and Separation of Duties

PURPOSE:

This appendix is provided to describe industry best security practices for assigning separate administrator accounts to support the concept of Least Privilege.

ATTRIBUTION:

- SANS, “The Critical Security Controls for Effective Cyber Defense”, version 5.0
- NIST SP 800-53, “Security and Privacy Controls for Federal Information Systems and Organizations”, Revision 4 dated April 2013
- NIST SP 800-12, “An Introduction to Computer Security: The NIST Handbook” dated October 1995
- CNSSI-4009, “National Information Assurance (IA) Glossary”, dated April 2010

DEFINITIONS:

Least Privilege – The principle that security architecture be designed to grant individual users and processes only the minimum accesses to system resources and authorizations required to perform their official duties or function.

Separation of Duties – The security principle requiring the division of roles and responsibilities so that a single individual cannot subvert a critical process or function.

SUMMARY:

The implementation of least privilege is accomplished by assigning user or process access to system resources based on operational or business needs. Thus, access is granted to only those resources required to perform assigned duties. For individuals who have multiple roles within the organization requiring varying levels privileges, this assignment of access can be challenging. Often times the agency will assign a single userid to the individual and elevate the privileges for that account based on the different roles. While it may seem logical to allow the user access to all

required resources using a single account, security vulnerabilities can be introduced into the system.

Associated with least privilege is separation of duties. This concept aids in maintaining the integrity of the system by preventing the abuse of elevated privileges for making unauthorized changes to the system. This objective essentially requires different individuals to perform separate functions with relation to (primarily) administrative duties. For instance, those with the ability to create and assign user access to system should not be able to access the audit logs that contain the evidence of the account actions.

USER ACCESS AND ACCOUNT MANAGEMENT:

Several factors influence the manner in which an agency implements and manages user access. Many times, the size of the agency and the technical expertise of the IT staff employed by the agency become primary drivers. Larger agencies with a broad base of technically savvy personnel normally have the ability to dedicate resources specifically to the administration and management of user access. This could translate to the use of multiple accounts for a single user performing duties requiring varying levels of access.

Smaller agencies with few or no technically experienced personnel will often assign single user accounts with the highest level of access required by users. Other smaller agencies may go as far as assigning every user an account with elevated privileges so there are no delays or problems requiring intervention by already overburdened system administrators. It is not uncommon for a smaller agency to outsource system administration duties.

Regardless of the size or resources of an organization, each agency should base the process for assigning access to system resources based on their operational requirements and a thorough risk assessment. To mitigate risk for accessing system resources, industry best security practices prescribe those individuals performing duties requiring elevated privileges be assigned a separate userid to be used in the performance of those duties. This account would be separate from a standard user account.

Why are some agencies unwilling to implement controls for least privilege? One common reason/perception is administrative overhead. There is a time factor for a system administrator to create user accounts and configure those accounts correctly based on the user's role. In larger agencies with many employees, this could add up to a significant impact on the system administrator(s) especially if there is a high level of turnover. Resources in some agencies may allow for a single system administrator dedicated strictly for account management. On the other end of the spectrum, in agencies with fewer employees, the impact may be more burdensome. While there are fewer user accounts to manage, a full-time system administrator for account

management may not be feasible. Those duties then become shared between a few people or added to the duties of a lone person.

Another reason may be the burden on system administrators to remember multiple userids and passwords. This could result in the user using the same password for each account or the user writing down the credentials for ease of remembrance. Additionally, an administrator could get the credentials mixed up between accounts causing an account lockout. This could then require system administrator intervention to reset or unlock the account.

Some agencies may feel that creating additional accounts reduces system resources. Depending on the size of the agency, this could be a concern. In most cases, the number of individuals that would require a secondary account would be minimal. The impact could be limited to a slight increase in disk space usage on the systems accessed by the system administrators with the separate accounts and perhaps the server housing the account information.

THREATS:

A primary goal of attackers is to gain administrative or root privileges on a network or system. Therefore, protection of credentials with that level of access is a key to preventing unauthorized access. Attackers may use many methods in attempts to gain unauthorized, privileged access to computer or network systems. There are two common techniques that take advantage of improperly managed administrative privileges.

Phishing Attacks

In this first method, consider a small organization with limited system administrative resources. Each user is assigned an account with elevated privileges that allows them to perform a myriad of duties including gaining access to critical system security resources. Because this is the only account the user has, normal non-administrative duties are also performed with administrative rights. While checking their email, the user is fooled into reading a message and opening a malicious attachment. Because the user's account has elevated privileges, malware is now installed on the system with elevated privileges. The malware could now allow the attacker to take over the system and install other malicious software such as key loggers, sniffers, or remote control applications. Other key system resources such as firewalls, routers, switches, or intrusion detection systems are now also compromised.

Password Brute Force Guessing / Cracking

The second method may not be as easy as the first and involves the guessing or cracking of passwords on the part of the attacker. Based on human nature, we tend to develop passwords that

are easy to remember and most likely contain some kind of information that is pertinent to us. Some passwords could be easily guessed with a minimal amount of social engineering or fact finding. Consider again an agency that assigns users a single account to perform all duties including those requiring elevated privileges. A user has created a password that, while meeting the requirements of the CJIS Security Policy, is comprised of easily guessed information about the user. An attacker has previously determined the userid and is now able to begin guessing the password. Upon success, the attacker will have unauthorized access to critical system resources.

MITIGATION:

The first step to implementing least privilege is to create separate user accounts for those individuals that require elevated privileges for their duties. These duties could include system or security administration, reviewing audit logs, backup administration, or configuring network devices (e.g. firewalls, routers). The passwords associated with these accounts should have a higher level of complexity than an account without elevated privileges. By disassociating the access levels required for system administration functions from an individual's "everyday use account", should a password be compromised, access would be limited to that of a user with non-elevated privileges.

Second is to implement procedures to ensure accounts with elevated privileges are used only for those duties requiring the higher level of access. This would mean disabling or blocking access to email, web browsers, and other external facing connections. While technical processes are the preferred method of preventing the misuse of accounts with elevated privileges, written policies can be used in situations where technology does not support that type of account management.

Several governance organizations recognize the importance of the security value of Least Privilege. The Payment Card Industry (PCI) includes requirements in their Data Security Standards (DSS). The National Institute of Standards and Technology (NIST) addresses the concept of Least Privilege in its Special Publication (SP) 800-53 rev. 4. While not considered a governance organization, the System Administration, Networking, and Security (SANS) Institute publishes a list of the top 20 security controls which includes "Controlled Use of Administrator Privileges" at number 12. Although the actual security controls or required implementation may slightly differ, the concept is consistent across the groups. The actual controls from NIST and SANS are included here in this appendix.

NIST CONSIDERATIONS FOR LEAST PRIVILEGE:

NIST Special Publication 800-53 rev. 4 includes controls required for all systems under the Federal Information Security Management Act. The publication specifies the guidance for Least Privilege in the control catalog under the Access Control (AC) family and specifically as AC-6. While the NIST requirements are not enforceable under the CJIS Security Policy, they were the genesis of

the Policy and do provide a sound security baseline that can be leveraged by the criminal and noncriminal justice community. AC-6 is a key control having several enhancements which, when implemented, bolster the overall security of the information system by reducing the risk of compromise through the misuse or misconfiguration of access to system resources.

AC-6 Least Privilege

Control: The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Supplemental Guidance: Organizations employ least privilege for specific duties and information systems. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions. Organizations consider the creation of additional processes, roles, and information system accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational information systems. Related controls: AC-2, AC-3, AC-5, CM-6, CM-7, PL-2.

Control Enhancements:

(1) LEAST PRIVILEGE / AUTHORIZE ACCESS TO SECURITY FUNCTIONS

The organization explicitly authorizes access to [Assignment: organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information].

Supplemental Guidance: Security functions include, for example, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters. Security-relevant information includes, for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users. Related controls: AC-17, AC-18, AC-19.

Control Enhancements:

(2) LEAST PRIVILEGE / NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS

The organization requires that users of information system accounts, or roles, with access to [Assignment: organization-defined security functions or security-relevant information], use non-privileged accounts or roles, when accessing nonsecurity functions.

Supplemental Guidance: This control enhancement limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies such as role-based access control and where a change of role provides the same degree of assurance in the change of access authorizations for both the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account. Related control: PL-4.

(3) LEAST PRIVILEGE / NETWORK ACCESS TO PRIVILEGED COMMANDS

The organization authorizes network access to [Assignment: organization-defined privileged commands] only for [Assignment: organization-defined compelling operational needs] and documents the rationale for such access in the security plan for the information system.

Supplemental Guidance: Network access is any access across a network connection in lieu of local access (i.e., user being physically present at the device). Related control: AC-17.

(4) LEAST PRIVILEGE / SEPARATE PROCESSING DOMAINS

The information system provides separate processing domains to enable finer-grained allocation of user privileges.

Supplemental Guidance: Providing separate processing domains for finer-grained allocation of user privileges includes, for example: (i) using virtualization techniques to allow additional privileges within a virtual machine while restricting privileges to other virtual machines or to the underlying actual machine; (ii) employing hardware and/or software domain separation mechanisms; and (iii) implementing separate physical domains. Related controls: AC-4, SC-3, SC-30, SC-32.

(5) LEAST PRIVILEGE / PRIVILEGED ACCOUNTS

The organization restricts privileged accounts on the information system to [Assignment: organization-defined personnel or roles].

Supplemental Guidance: Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from having access to privileged information/functions. Organizations may differentiate in the application of this control enhancement between allowed privileges for local accounts and for domain accounts provided organizations retain the ability to control information system configurations for key security parameters and as otherwise necessary to sufficiently mitigate risk. Related control: CM-6.

(6) LEAST PRIVILEGE / PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS

The organization prohibits privileged access to the information system by non-organizational users.

Supplemental Guidance: Related control: IA-8.

(7) LEAST PRIVILEGE / REVIEW OF USER PRIVILEGES

The organization:

(a) Reviews [Assignment: organization-defined frequency] the privileges assigned to [Assignment: organization-defined roles or classes of users] to validate the need for such privileges; and

(b) Reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.

Supplemental Guidance: The need for certain assigned user privileges may change over time reflecting changes in organizational missions/business function, environments of operation, technologies, or threat. Periodic review of assigned user privileges is necessary to determine if the rationale for assigning such privileges remains valid. If the need cannot be revalidated, organizations take appropriate corrective actions. Related control: CA-7.

(8) LEAST PRIVILEGE / PRIVILEGE LEVELS FOR CODE EXECUTION

The information system prevents [Assignment: organization-defined software] from executing at higher privilege levels than users executing the software.

Supplemental Guidance: In certain situations, software applications/programs need to execute with elevated privileges to perform required functions. However, if the privileges required for execution are at a higher level than the privileges assigned to organizational users invoking such

applications/programs, those users are indirectly provided with greater privileges than assigned by organizations.

(9) LEAST PRIVILEGE | AUDITING USE OF PRIVILEGED FUNCTIONS

The information system audits the execution of privileged functions.

Supplemental Guidance: Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised information system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing the use of privileged functions is one way to detect such misuse, and in doing so, help mitigate the risk from insider threats and the advanced persistent threat (APT). Related control: AU-2.

(10) LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS

The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

Supplemental Guidance: Privileged functions include, for example, establishing information system accounts, performing system integrity checks, or administering cryptographic key management activities. Non-privileged users are individuals that do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.

References: None.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD AC-6 (1) (2) (5) (9) (10)	HIGH AC-6 (1) (2) (3) (5) (9) (10)
----	------------------	-------------------------------	------------------------------------

**SYSTEM ADMINISTRATION, NETWORKING, AND SECURITY (SANS)
CONSIDERATION FOR LEAST PRIVILEGE:**

There are many negative factors that affect our cyber lives: massive data loss, intellectual property theft, credit card breaches, and identity theft just to name a few. Cyber defense is rapidly evolving to address the plethora of challenges we face. Defenders have access to a wide array of resources to combat those wishing to do harm. Ranging from the collection of vast amounts of intelligence data to security standards to training and certifications, security practitioners are well armed.

But can information overload actually worsen the problem? Organizations must decide, hopefully based on risk analysis, how to wade through all available resources and select those best suited to their own operating environment. The threats continue to evolve, the attackers become smarter, and user access more mobile. The cloud beckons and can provide reduced cost and infrastructure at a price of less control and accountability for vital information.

The SANS Institute publishes the “20 Critical Security Controls for Effective Cyber Defense”. This list of controls is the combined result of work by an international community to create, adopt, and support the controls. The components of the community provide insight, tools, information, and solutions into threats and adversaries. This list includes the control titled “Controlled Use of Administrative Privileges”. SANS describes this control as: *The process and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.*

Critical Security Control (CSC) 12: Controlled Use of Administrative Privileges

The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

ID #	Description	Category
CSC 12--1	Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.	<i>Quick win (One of the “First Five”)</i>
CSC 12--2	Use automated tools to inventory all administrative accounts and validate that each person with administrative privileges on desktops, laptops, and servers is authorized by a senior executive	<i>Quick win</i>
CSC 12--3	Configure all administrative passwords to be complex and contain letters, numbers, and special characters intermixed, and with no dictionary words present in the password. Pass phrases containing multiple dictionary words, along with special characters, are acceptable if they are of a reasonable length.	<i>Quick win</i>

CSC 12--4	Before deploying any new devices in a networked environment, change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration--level accounts.	<i>Quick win</i>
CSC 12--5	Ensure that all service accounts have long and difficult--- to--- guess passwords that are changed on a periodic basis, as is done for traditional user and administrative passwords.	<i>Quick win</i>
CSC 12--6	Passwords should be hashed or encrypted in storage. Passwords that are hashed should be salted and follow guidance provided in NIST SP 800--132 or similar guidance. Files containing these encrypted or hashed passwords required for systems to authenticate users should be readable only with super---user privileges.	<i>Quick win</i>
CSC 12--7	Utilize access control lists to ensure that administrative accounts are used only for system administration activities, and not for reading e---mail, composing documents, or surfing the Internet. Web browsers and e---mail clients especially must be configured to never run as administrator.	<i>Quick win</i>
CSC 12--8	Through policy and user awareness, require that administrators establish unique, different passwords for their administrative and non---administrative accounts. Each person requiring administrative access should be given his/her own separate account. Users should only use the Windows “administrator” or UNIX “root” accounts in emergency situations. Domain administration accounts should be used when required for system administration instead of local administrative accounts.	<i>Quick win</i>
CSC 12--9	Configure operating systems so that passwords cannot be re--- used within a timeframe of six months.	<i>Quick win</i>
CSC 12--10	Configure systems to issue a log entry and alert when an account is added to or removed from a domain administrators’ group, or when a new local administrator account is added on a system.	<i>Visibility/ Attribution</i>
CSC 12--11	Configure systems to issue a log entry and alert when unsuccessful login to an administrative account is attempted.	<i>Visibility/ Attribution</i>

CSC 12--12	Use multifactor authentication for all administrative access, including domain administrative access. Multi-factor authentication can include a variety of techniques, to include the use of smart cards with certificates, One Time Password (OTP) tokens, and biometrics.	<i>Configuration/ Hygiene</i>
CSC 12--13 (NEW)	When using certificates to enable multi-factor certificate-based authentication, ensure that the private keys are protected using strong passwords or are stored in trusted, secure hardware tokens.	<i>Configuration/ Hygiene</i>
CSC 12--14	Block access to a machine (either remotely or locally) for administrator-level accounts. Instead, administrators should be required to access a system using a fully logged and non-administrative account. Then, once logged on to the machine without administrative privileges, the administrator should transition to administrative privileges using tools such as Sudo on Linux/UNIX, RunAs on Windows, and other similar facilities for other types of systems. Users would use their own administrative accounts and enter a password each time that is different than their user account.	<i>Configuration/ Hygiene</i>

Quick win: Implementation provides significant risk reduction without major financial, procedural, architectural, or technical changes to an environment, or that provide substantial and immediate risk reduction against very common attacks that most security-aware organizations prioritize these key controls.

Visibility / attribution: Measures to improve the process, architecture, and technical capabilities of organizations to monitor their networks and computer systems to detect attack attempts, locate points of entry, identify already-compromised machines, interrupt infiltrated attackers' activities, and gain information about the sources of an attack.

Configuration / hygiene: reduce the number and magnitude of security vulnerabilities and improve the operations of networked computer systems, with a focus on protecting against poor security practices by system administrators and end-users that could give an attacker an advantage.

SEPARATION OF DUTIES:

Separation of duties is another security control related to least privilege. Many of the same challenges faced by least privilege apply to this concept as well. Agency size and resources play a major in the implementation of separation of duties. As the name implies, some key functions should be separated between different individuals. The goal of this concept is to provide protection

against a single individual's ability to circumvent system security controls to gain unauthorized access or perform unauthorized actions without colluding with other individuals.

Simply put separation of duties entails distributing certain critical mission oriented functions or system administrative support functions amongst different individuals or roles. It also includes delineating information system support duties such as auditing, configuration control, or network security between different individuals.

As with least privilege, an agency's ability to implement separation of duties is typically based on financial and personnel resources. While a very large agency may have ready availability to those resources to ensure critical functions are spread across multiple individuals, a small agency probably does not have that luxury.

THREATS:

What effect can an individual with carte blanc access to all critical functions of a system have? Consider a single individual with the ability to install nefarious applications on a system (e.g. a keylogger). If this same individual also has the ability to edit any audit logs that would have recorded the actions of installing the software, those entries could be deleted and any evidence of the installation eliminated.

Perhaps a disgruntled system administrator wants to open a port on a firewall to allow a remote backdoor connection into the information system in order to siphon off criminal justice information. Because the perpetrator has access to the firewall and all logs, the port can be opened and the logs tampered with to eliminate records of the action.

As mentioned previously, the two concepts of least privilege and separation of duties are related. Additional threats are presented when a system administrator using a single account with unlimited elevated privileges across the information system uses that account to check email. In a successful phishing attack that compromises this account, the attacker now has unrestricted unauthorized access to all system resources and the ability to hide their tracks.

MITIGATION:

The primary method to avoid these situations is to configure system privileges and duties such that a single person is unable to effect questionable change to the system and then are able to erase any evidence of the change.

Technical configurations are most secure and sound enforceable policies compliment the technical solutions. When an information system does not support separating duties, strong policies help mitigate risk.

NIST CONSIDERATIONS FOR SEPARATION OF DUTIES:

NIST Special Publication 800-53 specifies the guidance for separation of duties in the control catalog under the Access Control (AC) family and specifically as AC-5. While the NIST requirements are not enforceable under the CJIS Security Policy, they were the genesis of the Policy and do provide a sound security baseline that can be leveraged by the criminal and noncriminal justice community. AC-5 is a relatively small control with no enhancements but it is significant in protecting the integrity of an information system.

AC-5 Separation of Duties

Control: The organization:

- a. Separates [*Assignment: organization-defined duties of individuals*];
- b. Documents separation of duties of individuals; and
- c. Defines information system access authorizations to support separation of duties.

Supplemental Guidance: Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions. Related controls: AC-3, AC-6, PE-3, PE-4, PS-2.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD AC-5	HIGH AC-5
----	------------------	----------	-----------

G.6 Encryption

Encryption

Purpose:

This paper was created to provide assistance and guidance on encryption types, methods, and to provide general best practices in the implementation of encryption.

Attribution:

- FIPS 140 – 2, Security Requirements for Cryptographic Modules (May 2001)
- FIPS 197, Advanced Encryption Standard (Nov 2001)
- NIST SP 800-111, Guide to Storage Encryption Technologies for End User Devices
- CNSSP-15, National Information Assurance Policy on the Use of Public Standards for Secure Sharing of Information among Security Systems
- CJIS Security Policy

Definitions and Terms:

Encryption – A form of cryptology that applies a cryptographic operation to provide confidentiality of (sensitive) information.

Decryption – The inverse cryptographic operation used to convert encrypted information back into a plaintext (readable) format.

Asymmetric Encryption – A type of encryption that uses key pairs for encryption. One key is used to encrypt a message and another key to decrypt the message. Asymmetric encryption is also commonly known as public key encryption.

Symmetric Encryption – A type of encryption where the same key is used to encrypt and decrypt a message. Symmetric encryption is also known as secret key encryption.

Hybrid encryption – A type of encryption where both asymmetric encryption and symmetric encryption keys are used creating what is referred to as cipher suites. In a hybrid solution the asymmetric encryption keys are used for client/server certificate exchange to provide session integrity while the symmetric encryption keys are used for bulk data encryption to provide data confidentiality.

Authorized User/Personnel - An individual, or group of individuals, who have been appropriately vetted through a national fingerprint-based record check and have been granted access to CJI.

Summary:

CJIS Security Policy encryption requirements are intended to provide protection of the sensitive data that is criminal justice information (CJI). The primary goal of encrypting CJI is to prevent unauthorized access to this sensitive data. Encryption is a great tool that can be applied to accomplish this protection and ensure compliance with the vast majority of the CJI requirements. CJIS Security Policy Section 5.10.1.2 details when encryption is required and provides information on the exceptions to the encryption requirement.

Achieving CJIS Security Policy Compliance:

To determine when encryption is required one must first read and understand CJIS Security Policy Section 5.9.1 Physically Secure Location. The reason for this is simple: encryption is not required while within a physically secure location. Conversely, whenever CJI is transmitted or stored (at rest) outside the boundaries of a physically secure location encryption may be required. The exact standards to which the data would be required to meet are detailed along with any exceptions in CJIS Security Policy Section 5.10.1.2.

Additionally, both security awareness training and personnel security requirements can be affected by whether or not CJI is encrypted. Requirements surrounding these Policy areas is determined by answering the following question: Who has unescorted access to unencrypted CJI?

Unless personnel is escorted, security awareness training is required as correlated with the access level needed by personnel as identified in CJIS Security Policy Section 5.2. Similarly, fingerprint-based background checks as detailed in CJIS Security Policy Section 5.12 may be required on individuals to permit unescorted access to CJI.

The intent of all these requirements is to limit access to CJI to only authorized personnel. CJIS Security Policy Appendix A: Terms and Definitions defines authorized user/personnel as an individual, or group of individuals, who have been appropriately vetted through a national fingerprint-based record check and have been granted access to CJI.

What is Encryption?

Encryption is the process of encoding messages or information in such a manner that only people with the knowledge or means to decrypt the message can do so. But how does this work?

In an encryption process, legible data, referred to as plaintext, is encrypted by applying a cipher (otherwise known as an encryption algorithm or crypto key) to the data. The data then becomes encrypted and is now referred to as ciphertext. The ciphertext is essentially unreadable until decrypted. The decryption process requires the process of applying the same algorithm (crypto key) to encrypt the data in an inverse manner to convert the data back into plaintext.

Encryption is important because it allows you to securely protect data that you don't want anyone else to have access to. Encryption has been used throughout history to send “secrets” securely by some form of obfuscation to a recipient. Businesses and enterprises use encryption to protect corporate secrets and sensitive employee data, such as payroll information and personally identifiable information (PII). Governments secure classified information with encryption. Additionally, individuals may use encryption to protect personal information, such as credit card data, banking information, and passwords to guard against things like identity theft.

It should be known that encryption may not always prevent the interception of data. If the stolen data is encrypted, though, it would be extremely difficult for any of the data to be decrypted without having the decryption key. While it may be possible to decrypt the message without possessing the key, it does require large computational resources, great skill, and lots of time to accomplish such a task. Exercising encryption along with key management policies is one of the best security practices that can be put into place with regard to sensitive data security and protection.

Types of Encryption:

Symmetric Encryption

Symmetric encryption is also commonly known as secret key encryption. Symmetric encryption is a form of cryptography utilizing a singular encryption key to guise an electronic message. Its data conversion uses a mathematical algorithm along with a secret key, which results in the inability to make sense out of a message. Symmetric encryption is a two-way algorithm because the mathematical algorithm is reversed when decrypting the message along with using the same secret key.

Symmetric encryption is most often used for data protection whether at rest or in transit, especially in bulk, due to the ease and speed with which the encryption can be implemented. The most common examples of symmetric algorithms are: AES and Triple-DES (3DES or TDEA).

How it works:

To encrypt and send a message to Jane, John does the following:

1. Generates a new symmetric key
2. Encrypts the message using this new symmetric key
3. Sends the message to Jane
4. Sends the encrypted symmetric key to Jane - out of band

To decrypt this ciphertext, Jane does the following:

1. Receives the encrypted message
2. Receives the symmetric key
3. Uses the symmetric key to decrypt the message

Asymmetric Encryption

Asymmetric encryption is also commonly known as public-key encryption. Asymmetric cryptography is cryptography in which a pair of keys, a public key and a private key, are used to encrypt and decrypt a message so that it arrives securely. Initially, a network user receives a public and private key pair from a certificate authority. Any other user who wants to send an encrypted message can get the intended recipient's public key from a public directory. They use this key to encrypt the message, and they send it to the recipient. When the recipient gets the message, they decrypt it with their private key, which no one else should have access to.

Creating Key Pairs:

Asymmetric encryption requires the use of algorithms of great computational complexity to create the key pairs. This is accomplished by using a large, random number that an algorithm is applied to which generates a pair of keys for use as asymmetric key algorithms (as shown in Figure 1 below).

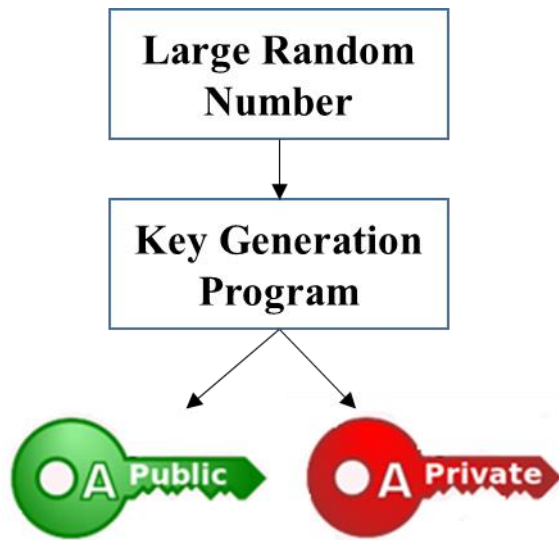


Figure 1 – Asymmetric key pair generation

Asymmetric encryption is most often used to encrypt a single message before transmission. The most common examples of asymmetric algorithms are: RSA and DSA.

How it works:

To encrypt and send a message to Jane, John does the following:

1. Obtains Jane's public key
2. Encrypts the message using Jane's public key
3. Sends the message to Jane

To decrypt this ciphertext, Jane does the following:

1. Receives the encrypted message
2. Uses her private key to decrypt the message

Advantages of Using Symmetric Encryption for Data Protection

Asymmetric encryption requires the use of algorithms with great computational complexity to create the key pairs, and therefore is not practical for large amounts of data. It is typically used for only for short messages. Also, asymmetric encryption must use a comparatively stronger key than symmetric key encryption to achieve the same level of protection as one key (public) will be published in the public directory for all to see.

Symmetric encryption is based on large, but simple algorithms which require less computation. Therefore, is much faster to create and use keys. This allows the same key to be used to encrypt and decrypt the message. So, data can be encrypted in real time. The (shared) key is sent to the recipient out of band so that it can be used to decrypt the data.

For the reasons stated above, symmetric key encryption is the preferred choice by both industry and government alike to encrypt large amounts of data (bulk encryption) simply due to the ease and real time encryption capabilities as detailed above. Additionally, a new key can be generated for every session, message transaction, etc., as desired. This means a sender won't have to use one key (public) to encrypt a message and have the recipient use another key (private) to decrypt the message.

Hybrid Encryption

Hybrid encryption solution exist where both asymmetric encryption and symmetric encryption keys are used to create what is referred to as cipher suites. In a hybrid solution the asymmetric encryption keys are used for client/server certificate exchange to provide session integrity while the symmetric encryption keys are used for bulk data encryption to provide data confidentiality.

Hybrid solutions are most often used by Internet browsers to protect data in transit. The most common examples of hybrid encryption are: TLS/SSL, PGP, IPSEC, and S/MIME.

How it works:

To encrypt a message to Jane in a hybrid cryptosystem, John does the following:

1. Obtains Jane's public key
2. Generates a new symmetric key
3. Encrypts the message using this new symmetric key
4. Encrypts the symmetric key using Jane's public key
5. Sends the message to Jane

To decrypt this hybrid cipher text, Jane does the following:

1. Receives the encrypted message
2. Receives the encrypted symmetric key
3. Uses her private key to decrypt the symmetric key
4. Uses the symmetric key to decrypt the message

Explaining Cipher Suites:

A cipher suite is a set of cryptographic algorithms used for the following:

- Protect information required to create shared keys (key exchange)
- Encrypt messages exchanged between clients and servers (bulk encryption)
- Generate message hashes and signatures to ensure the integrity of a message (message authentication)

Examples of Transport Layer Security (TLS) 1.2 Cipher Suites:

- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256

A cipher suite specifies one algorithm for each of the above tasks. For example, the TLS_RSA_WITH_AES_128_SHA256 cipher suite is used for TLS. The suite uses the RSA asymmetric algorithm for key exchange, AES with a 128-bit key for bulk data encryption, and SHA256 for message authentication.

Symmetric and Asymmetric Key Strength Comparison:

<u>Symmetric</u>		<u>Asymmetric</u>		
<u>Bits of security</u>	<u>Symmetric key algorithms</u>	<u>Finite-Field Cryptography (FFC)</u> <u>(e.g., DSA, D-H)</u> <u>Bits of security</u>	<u>Integer-Factorization Cryptography (IFC)</u> <u>(e.g., RSA)</u> <u>Bits of security</u>	<u>Elliptic-Curve Cryptography (ECC)</u> <u>(e.g., ECDSA)</u> <u>Bits of security</u>
<u>80</u>	<u>2TDEA18</u>	<u>Public key = 1024</u> <u>Private key = 160</u>	<u>Key size = 1024</u>	<u>Key size = 160-223</u>
<u>112</u>	<u>3TDEA</u>	<u>Public key = 2048</u> <u>Private key = 224</u>	<u>Key size = 2048</u>	<u>Key size = 224-255</u>
<u>128</u>	<u>AES-128</u>	<u>Public Key = 3072</u> <u>Private key = 256</u>	<u>Key size = 3072</u>	<u>Key size = 256-383</u>
<u>192</u>	<u>AES-192</u>	<u>Public key = 7680</u> <u>Private key = 384</u>	<u>Key size = 7680</u>	<u>Key size = 384-511</u>
<u>256</u>	<u>AES-256</u>	<u>Public key = 15360</u> <u>Private key = 512</u>	<u>Key size = 15360</u>	<u>Key size = 512+</u>

Figure 2 - Symmetric and asymmetric key strength comparison

As you can see in the chart provided above, the equivalent key strengths between symmetric and asymmetric key strengths do not necessarily correlate. There is a reason for this. As stated previously, asymmetric algorithms must use a comparatively stronger key than symmetric key encryption to achieve the same strength. The simplest explanation for this is because one of the keys is published to the public directory and can constantly be attacked by anyone with access to the directory. Therefore, the public key must be made of such strength that it can resist getting compromised while made public.

Federal Information Processing Standard (FIPS) 140-2 Explained

Origin of FIPS 140-2

On July 17, 1995, the National Institute of Standards and Technology (NIST) established the Cryptographic Module Validation Program (CMVP) to validate cryptographic modules to Federal Information Processing Standards (FIPS) Security Requirements for Cryptographic Modules, and other FIPS cryptography based standards. The CMVP is a joint effort between NIST and the Communications Security Establishment Canada (CSEC). FIPS 140-2, Security Requirements for Cryptographic Modules, was released on May 25, 2001 to supersede the original FIPS 140-1. Modules validated as conforming to FIPS 140-1 and FIPS 140-2 are accepted by the Federal Agencies of both countries for the protection of sensitive information.

What is FIPS 140-2?

Federal Information Processing Standard (FIPS) is a standard developed and recommended (often mandated) for use in federal-government-operated IT systems by the following two government bodies:

- The National Institute of Standards and Technology (NIST) in the United States
- The Communications Security Establishment (CSE) in Canada

FIPS 140-2 specifies the security requirements a cryptographic module must meet when utilized within a security system protecting sensitive information within information systems (computer and telecommunication systems). FIPS 140-2 specifies which encryption algorithms can be used and how encryption keys are to be generated and managed.

How does a product get certified?

Vendors of cryptographic modules can have their products tested by independent, accredited Cryptographic and Security Testing (CST) laboratories. The CST laboratories use the Derived Test

Requirements (DTR), Implementation Guidance (IG) and applicable CMVP programmatic guidance to test cryptographic modules against the applicable standards in a variety of implementations. The result of these tests are reported to NIST's Computer Security Division (CSD) and CSEC who jointly serve as the Validation Authorities for the program. These results are then reviewed and certificates would be issued if the results are determined to be acceptable.

What is the difference between being FIPS 140-2 compliant and being FIPS 140-2 certified?

It is common theme to discover a product is “FIPS compliant.” What does this mean, though? The difference between compliance and certification is not subtle. Certification requires a vast testing, verification, and validation process be performed by a CST laboratory as described in the previous section. Compliance is merely a claim stating the implementation of an encryption solution is done in accordance with the security policy related to the FIPS certification. Any claim of compliance would need to be validated and the corresponding certificate number would have to be known.

NIST has addressed related claims as shown below in their Frequently Asked Questions for the Cryptographic Module Validation Program:

A vendor makes the following claims of conformance to FIPS 140-2. Are they acceptable?

- The module has been designed for compliance to FIPS 140-2. <NO>
- Module has been pre-validated and is on the CMVP pre-validation list. <NO>
- The module will be submitted for testing. <NO>
- The module has been independently reviewed and tested to comply with FIPS 140-2. <NO>
- The module meets all the requirements of FIPS 140-2. <NO>
- The module implements FIPS Approved algorithms; including having algorithm certificates. <NO>
- The module follows the guidelines detailed in FIPS 140-2. <NO>
- The module has been validated and has received Certificate #XXXX. <YES>

A cryptographic module does not meet the requirements or conform to the FIPS 140-2 standard unless a reference can be made to the validation certificate number. The module used must also be the same version/part number as annotated on the validation certificate. Any other claims are not relevant.

To read more FAQs from NIST on FIPS certification, use the following NIST website link:
<http://csrc.nist.gov/groups/STM/cmvp/documents/CMVPFAQ.pdf>

Where can I learn more about FIPS 140-2?

For more information about the FIPS 140-2 standard, go to the following NIST website:
<http://csrc.nist.gov/cryptval/140-2.htm>

General Recommendations:

Encryption key management control is of paramount importance! Agencies should develop policies and procedures define and monitor the administrative tasks involved with protection, storage, organization, access controls and the lifecycle management of encryption keys. After all, encryption keys should not be accessible by just anyone. An encryption key management control process should ensure only authorized users have access to encryption keys. Key management is a best security practice and helps to ensure the confidentiality and integrity of CJI data and enforces key access control.

The CJIS Security Policy is a “living” document under constant review and receiving regular updates through the Advisory Policy Board (APB) process. Agencies need to always keep up to date on the latest requirements. These requirements can be found in CJIS Security Policy Section 5.10.1.2. Please contact the CJIS ISO Program anytime to address any questions or concerns about CJIS Security Policy requirements, the current APB status of CJIS Security Policy requirements, or if seeking general information or guidance.

G.7 Incident Response

Incident Response

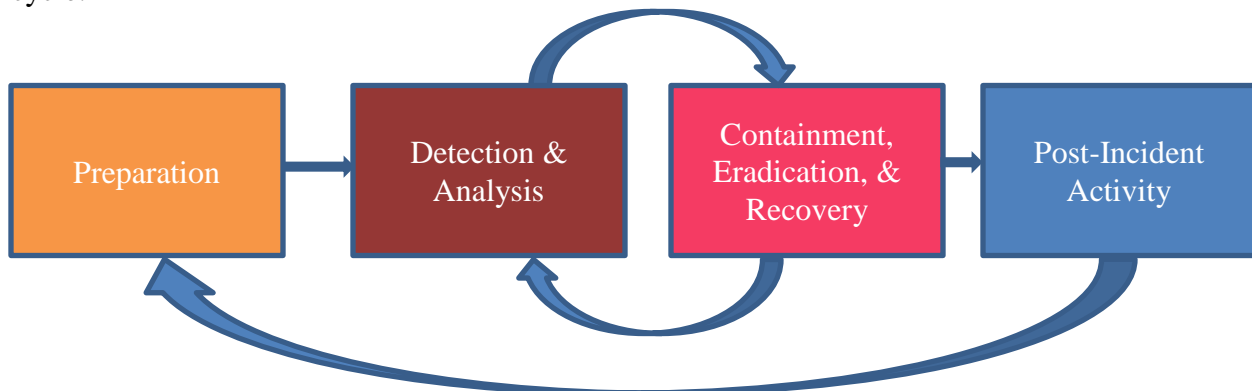
Introduction

Information technology (IT) security incident response is an important and critical component of information technology programs. Performing incident response effectively can be a complex undertaking – for that reason, establishing a successful incident response capability requires planning and resources. Everyone in an organization must be aware of IT security risks, threats, and actions to take in situations where an actual IT security incident has occurred. Even the best-secured and controlled environments can experience these security risks, threats, events, and incidents. This document provides guidelines for appropriate response to IT security incidents, and are independent of specific hardware platforms, operating systems, protocols, or applications.

The following example incidents are used to highlight appropriate actions during each phase:

- Malicious code execution
- Ransomware execution
- Denial of service attack
- Social Engineering
- Phishing

NIST Special Publication 800-61 rev. 2 outlines the “Incident Response Life Cycle” as a collection of phases – distinct sets of activities that will assist in the handling of a computer security incident, from start to finish. The following diagram explains the process flow of the incident response life cycle:



Preparation

The initial phase of the incident response life cycle, “Preparation”, involves establishing and training an incident response team, and acquiring the necessary tools and resources. A computer security incident may not have happened at this phase, but it is important to utilize all available knowledge and security measures to obtain the best posture for responding to potential future incidents. One of the most important preparation steps involves the collection, storage, and accessibility of event data and telemetry from hardware and software resources such as firewall logs, application logs, operating system logs, and other valuable sources of situational data, as well as the output of products that perform analysis on such data. Preventive measures to mitigate or eliminate future incidents are deployed during this phase, using industry best practices, data obtained from research and intelligence sources, and lessons learned from past incidents.

It is also imperative to prepare a list of contact information or notification methodologies to employ when an incident occurs, as well as notification and communication strategies within the team, with stakeholders, and with upper management and potentially other criminal justice and non-criminal justice agencies. This will help ensure that when incidents arise, the proper personnel and organizations are notified and kept informed of the circumstances regarding the incident.

Using the example incident categories outlined earlier, some overview into appropriate actions and activities for the Preparation phase can be given:

Malicious code execution

Preparation for incidents involving malicious code execution should initially involve user awareness of sources of malicious code. There are many potential sources of malicious code, such as web pages, emails, and removable media. The utilization and deployment of effective antivirus software, integrity-monitoring software, and intrusion detection and prevention software are effective measures to take to prepare for incidents involving malicious code execution.

Ransomware execution

Preparation phase activities for incidents involving ransomware execution are much the same as activities for malicious code execution, as ransomware is a specialized form of malware that encrypts potentially important or critical files, with the intention of coercing a victim to pay for a decryption key. Implementing a robust offline backup solution for these types of files is an important preparative action to take regarding the execution of ransomware. This will ensure that when ransomware attacks do happen, the mission impact is as minimal as possible and very little or no data is lost.

Denial of service attack

Denial of service attacks are given attention in the preparation phase. Defensive responses to denial of service attacks typically involve the use of a combination of attack detection and traffic classification and response tools, aiming to block traffic identified as abusive denial of service activity. Deploying solutions such as IDS/IPS devices and software, network hardware with rate-limiting capabilities (routers, switches, and firewalls), and upstream filtering devices at the system perimeter can mitigate for denial of service attacks.

Social Engineering

Preparation for social engineering attacks starts with user awareness training. Understanding and identifying attempts to obtain information in an unauthorized manner is crucial to thwarting these types of scenarios. Social engineering is the art of manipulating people to obtain information they may not be authorized to handle. Training and routinely testing users on potential social engineering scenarios and tactics, and providing training regarding appropriate responses to requests involving personal or otherwise sensitive information (for example, passwords or criminal justice information), is an effective way to ensure social engineering attacks never traverse past the preparation phase of the incident response life cycle.

Phishing

Like social engineering, preparation for phishing attacks is imperative. Phishing is a social engineering technique attackers employ to deceive users, in a fraudulent attempt to obtain sensitive information, or to gain unauthorized access to systems. Phishing is extremely widespread, and attackers disguising fraudulent scenarios in electronic communication such as email and instant messages are the most common. User awareness of these types of tactics is paramount to prepare for phishing attacks and schemes.

Detection and Analysis

The detection and analysis phase begins when a security incident has occurred. To understand when this phase begins, there must be a capability for an intelligent determination of circumstances constituting a security incident. Specialized knowledge and highly trained personnel are necessary for this step to be effective. Many organizations employ teams of personnel who are specifically trained to handle the intricacies of the incident response life cycle. The determination of a security incident can arise from one or several circumstances simultaneously – for example:

- Trained personnel manually reviewing collected event data for evidence of compromise
- Software applications analyzing events, trends, and patterns of behavior
- The observation of suspicious or anomalous activity on a computer system

The goals of this phase are:

- To detect whether a security incident occurred
- To determine the vector (i.e., method) of attack
- To determine the impact of the incident to the mission, systems, and personnel involved in the incident
- To obtain or create intelligence products regarding attack vectors and methodologies, especially when dealing with malicious code

Prioritization of incidents is also an important decision point in the incident response life cycle, as the circumstances regarding an incident can bring the situation to a critical level. There are three major impacts to consider when addressing priority of incidents:

- **Functional Impact:** the impact to business functionality
- **Information Impact:** the impact to confidentiality, integrity, and/or availability of criminal justice information
- **Recoverability:** the amount of time and resources that must be spent on recovering from an incident

Documentation regarding an incident should be thorough and applicable to the incident. This can be crucial in incidents that may lead to legal prosecution, as well as being invaluable to efficiently document, track, handle, manage, and resolve one or more incidents at the same time.

Using the example incident categories outlined earlier, some overview into appropriate actions and activities for the Detection and Analysis phase are given:

Malicious code execution

Detection of malicious code execution is often a primary job of host-based antivirus software. Having a capable and up-to-date antivirus solution installed on a system can detect known malicious code, as well as detect potentially malicious behaviors. The delivery of malicious code to a system can be detected by network traffic analysis and protection tools and hardware. Additionally, some malicious code may produce network traffic that is indicative of successful execution, exploitation, and/or compromise of a system. Solutions such as intrusion detection/prevention systems, Security Information and Event Management (SIEM) tools, and file integrity monitoring software can provide the necessary level of fidelity to make a determination of malicious code execution.

Knowing if or when a system is infected is not always immediately evident. Security controls may have been bypassed or even disabled by the malicious code. However, systems infected by malicious code or software (i.e. malware) can exhibit several indicators. These indicators include, but are not limited to:

Unexpected pop-up windows

- Slow start up and/or slow performance
- Suspicious hard drive activity including an unexpected lack of storage space
- Missing files
- Crashes and/or error messages
- Unexplained network activity
- Hijacked email

Analysis of malicious code can be performed in several ways. Static analysis of malicious code can be performed to determine the capabilities of the malicious code and generate actionable intelligence. Dynamic analysis of malicious code can be used to observe how the malicious code interacts with the system and what actions it performs and can often more rapidly determine the capabilities of malicious code. Both static and dynamic analysis can be performed manually, as well as in an automated fashion. Trained specialized personnel are crucial to the analysis of malicious code.

Ransomware execution

The detection of ransomware is identical to the detection of malicious code. Ransomware is specialized malicious code that encrypts potentially valuable files, generally with the intent to coerce a victim to pay a ransom for the possibility of the decryption of those files. Host-based antivirus solutions can also detect these threats, and network traffic analysis and protection tools and hardware can be used to prevent the successful execution of ransomware. SIEM tools and file integrity monitoring software can also detect the execution of ransomware.

Analysis of ransomware is identical to the analysis of malicious code, and the same intelligence can be determined in the same fashion as with the analysis of malicious code. The most obvious sign that ransomware has affected a system is the existence of encrypted files, the disappearance of certain types of files, and/or the presence of “ransom notes” on the system, which contain instructions for payment to obtain a decryption key, which may or may not be legitimate.

Denial of service attack

Denial of service (DoS) attacks are often detected at the perimeter of an organization but can also be detected within the organization as well. Often, from a user’s perspective, the signs of a DoS attack appear to be network performance or administrative maintenance related issues such as slow or broken network connections or down websites. Additionally, an administrator may notice ping time outs, event logs overflowing or alerts from network monitoring systems as issues that may identify a DoS attack. Intrusion detection and prevention software and platforms can detect denial of service attacks, as well as some network monitoring hardware and appliances, such as web application filters, routers,

firewalls, and switches. Devices targeted by denial of service attacks can also detect the attacks in some instances, if they have the capabilities to determine explicit attack activity versus normal network traffic.

Analysis of denial of service attacks include the determination of the source traffic, the protocols used to generate the traffic, the service(s) targeted by the attack, and the potential impacts of the attack. Network monitoring devices can often provide these types of data, with the exception of potential impacts of denial of service attacks on systems.

Social Engineering

Detection of social engineering attacks is primarily based on the situational awareness of the individual targeted by social engineering. Given that social engineering is a broad topic that can involve the manipulation and exploitation of people in control of an information system, user awareness of social engineering attempts is crucial. If the target has security awareness training in detecting attempts to gain information or access in an unapproved manner, social engineering is easier to detect.

Analysis of social engineering attacks will generally rely on the recollection abilities of or documentation taken by the targets of the attack. Social engineering may not occur on an information system and may be completely carried out in-person. If the target can recollect or produce documentation regarding the social engineering attempt, the motivation and desired access can potentially be determined. For successful social engineering attempts, recollection and documentation of the attempt is crucial to determining the level of unauthorized access that was obtained.

Phishing

Detection of phishing attacks generally will first occur at an organization's email point of presence. Some organizations still run their own email servers, and many have migrated to cloud solutions. Having an on-premise email server or server farm or cluster will require additional functionality to detect phishing attempts. For example, the header content of the email will need to be read, as well as the content inside the body of the email, to check for potentially malicious content and potentially falsified data that may indicate a phishing email. Many cloud email providers have built this capability into their email solutions, but it is still possible for users to receive phishing emails, as attacker tactics and capabilities evolve daily. The most effective detection of phishing comes from heightened situational awareness of potential attacks. Validating the source of the email can uncover potential phishing attempts.

Analysis of phishing attacks involves examination of email headers, as well as contents of the body of the email. The body of the email may contain malicious content, attachments, or links to suspicious or malicious content. Manual or automated analysis activities can be

performed on the email content. Analysis of these elements should be performed by trained specialized personnel to generate intelligence and aid with the determination of indicators of compromise.

Containment, Eradication, and Recovery

Containment activities for computer security incidents involve decision-making and the application of strategies to help control attacks and damage, cease attack activities, or reduce the impact or damage caused by the incident. Often, this requires intelligence gathered by the detection and analysis phases of the incident – for example, identification of affected hosts, identification of attacking hosts or attackers, identification of malware and its capabilities, and identification and monitoring of attacker communication channels can be invaluable to the implementation of containment activities. In most cases, it is important to introduce containment solutions all at once, as attackers may escalate their attack activity if deployment of the strategy is delayed.

Eradication efforts for a computer security incident involve removal of latent threats from systems (such as malware on the system and user accounts that may have been created), identifying and mitigating potential vulnerabilities or misconfigurations that may have been exploited, and identification of other hosts that may have been affected within the organization.

Recovery efforts for incidents involve restoration of affected systems to normal operation. This may include actions like restoring systems from backups, rebuilding systems from an agency-approved baseline, replacing compromised files with clean versions, installing patches, changing passwords, and increasing network perimeter and host-based security.

Compromised hosts are often attacked during these phases, as attackers try to regain their foothold on compromised systems or systems on the same network or others in the logical vicinity.

Malicious code execution

Containment activities for malicious code execution involve the logical or physical isolation of the host from the attacker's control and from any mission services or systems that would be impacted by the compromised host. This may include putting the host in a restricted VLAN, using firewalls to block traffic, disconnecting it from the network completely, shutting it down, or disabling functionality. Exercise caution as malicious code may have capabilities to take further actions on a host in case communications with a command and control server are severed. It is important to understand the capabilities of the malicious code before taking containment actions.

Eradication activities include the removal of malicious code from the system. This may be as simple as removing files, configuration rules, accounts, and other persistent items that the malicious code utilizes to function and maintain a presence on the system. This phase

also involves the discovery and removal of indicators of compromise on other systems, if applicable. It is imperative to remediate vulnerabilities that may have been exploited during eradication as well.

Recovery from malicious code execution generally is similar across many environments. Rebuilding the system from a clean baseline or restoring files from backup are typical activities that help restore the functionality of the system to continue the mission. Changing system passwords, installing patches, implementing tighter network access control, and ensuring appropriate levels of logging fidelity of the information system are integral parts of the recovery process.

Ransomware execution

Containment for ransomware execution should be as swift and immediate as possible, as ransomware can execute and spread to accessible media at a rapid pace. Considering files are being encrypted or have already been encrypted, immediate action should be taken to logically or physically isolate the system by disconnecting network connectivity. It is up to the system owner whether to take the risk in powering off the system, as valuable forensic artifacts may be destroyed in the process, but it will halt the execution of the ransomware and protect potentially valuable files. Please note that containment of active ransomware execution is one of the only circumstances where measures such as immediate shutdown are recommended.

Eradication of ransomware does not need to occur in most circumstances, as the entire goal of ransomware is to encrypt files and leave “recovery” instructions to extort victims. The vast majority of ransomware will delete itself once encryption of files is complete, but it is possible that some ransomware is persistent and can remain on the system. If this is the case, analysis should be performed on the ransomware to determine its capabilities, and eradication activities will proceed in an identical fashion to malicious code execution eradication activities.

Recovery from ransomware execution involves restoring encrypted files from backup and may involve the rebuilding of an entire system depending on the extent of the encryption from the ransomware. If a robust offline backup solution for hosts is not present or not utilized on a regular basis, the loss of potentially valuable data may be incredibly costly in several areas to repair, to include man-hours, revenue, and business products, data, and intelligence.

Denial of service attack

Containment of denial of service attacks involve the modification of access control where the attack is occurring. For example, if a web or application server is experiencing a denial of service attack, the system itself, as well as network monitoring devices, should be

examined to determine the source of the attack traffic. Once the source of the traffic is identified, modifications to access controls or rate-limiting features such as firewall access controls lists (ACLs) and web application filters can be employed to block the traffic. Care must be taken to determine if the observed traffic is actually intentional malicious denial of service traffic, versus heavy legitimate network traffic. Implementing access control mechanisms or rate-limiting features may negatively affect the mission of the system. It is also important to note that manual containment in this fashion may not be entirely effective, as attackers can circumvent the ACL by changing the attacking IP address, protocol, or other attribute of the connection.

Eradication is not necessarily applicable in denial of service scenarios, unless a vulnerability or misconfiguration is being exploited to cause the denial of service condition. If this is the case, take steps to remediate the vulnerability or misconfiguration.

Recovery actions depend on the available resources of the information system. For example, on-premise load balancers can be used to distribute the traffic, whether legitimate or malicious, to other less-burdened systems. Many cloud providers and content delivery networks also have denial of service mitigation capabilities. It may also be prudent to increase the resources (memory, processing capacity) of internet-facing systems so that they can handle larger amounts of traffic simultaneously.

Social Engineering

Containment regarding social engineering attacks is dependent upon the information or access that was provided to the attacker. For example, if an attacker gained access to an account on a system following a social engineering attempt, the account should be administratively disabled and all sources of event data regarding that account should be immediately collected. If sensitive data was divulged to the attacker, the impact of the exposure of that data should be examined and mitigating activity should be initiated to determine or reduce the damage of the spread of the information.

Eradication regarding social engineering attacks also depends on the information or access provided to the attacker. Removing or limiting the provided access is a pertinent eradication action. If the information provided is a credential to a system, disable and remove the credential from the system. Eradication may also involve the physical detainment or removal of personnel from a site.

Recovery actions for social engineering attacks are dependent on the information or access provided to the attacker. Additionally, security awareness training is an appropriate recovery action to ensure staff understands the threats of social engineering.

Phishing

Containment of phishing activity is tied very closely to the identification and analysis of the phishing activity. Understanding the tactics of the phishing attacker is paramount to deploying containment activities. Activities include, but are not limited to, administratively blocking sender email addresses and IPs, blocking potential malicious content in email via a web proxy, communicating with potential recipients, and implementation of email content or hyperlink blacklisting if possible. Phishing attacks can also include attempts to have users execute malicious code on systems, where containment activities regarding malicious code will be applicable.

Eradication of phishing attacks include the administrative removal of the emails from email systems, as well as eradication actions for malicious code if applicable.

Recovery from phishing attacks can include:

- Implementation and enforcement of the Domain Keys Identified Mail (DKIM) email authentication method, which can mitigate the possibility that attackers can send spoofed email
- Implementation and enforcement of Sender Policy Framework (SPF) to control and stop sender forgeries
- Implementation and enforcement of Domain-based Message Authentication, Reporting, and Conformance (DMARC), which enables message senders to indicate that their messages are protected with SPF and/or DKIM

Additionally, if malicious code is present in the phishing attack, recovery actions regarding malicious code may be applicable.

Post-Incident Activity

Post-incident activities occur after the detection, analysis, containment, eradication, and recovery from a computer security incident. Arguably one of the most important phases of incident response, post-incident activities involve the reflection, compilation, and analysis of the activities that occurred leading to the security incident, and the actions taken by those involved in the security incident, including the incident response team. Some of the important items to consider:

- Exactly what happened, and at what times?
- How well did staff and management perform in dealing with the incident?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?

- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar actions in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

Smaller incidents, and those that are similar to others that have been well documented, do not necessarily need much focus in this phase of incident response. Larger and less-understood security incidents should be the focus of a comprehensive post-mortem evaluation that outlines many of the items listed above and should include personnel that can have a direct impact on or are directly affected or responsible for the involved systems.

Post-incident activities such as these also help to serve as training opportunities for all parties involved in the incident, from victims, to system administration personnel, to incident responders.

Malicious code execution

Post-incident activities for malicious code execution generally will follow similar patterns. A timeline of activity should have been prepared using digital forensic data collected during the detection and analysis phases of the incident. This timeline should include all affected systems and times of all activities and actions taken during the incident. Steps that victims and system administrators may have taken during the course of the incident, as well as in close proximity to the time range of the incident, are valuable items to document and discuss. Any deviation from organizational policy should be noted and taken as training items or assigned consequences in accordance with organizational policies. It may also be pertinent to ensure that appropriate information and intelligence sharing was performed during and after the incident occurred. Corrective actions that may have prevented the execution of malicious code, such as antivirus solutions, restrictions on where executables can run, tightened permissions, and script blockers for browsers, should be considered as a mitigation for the risks posed by malicious code threats. Web proxy blocks from information discovered during analysis can be utilized to ensure that malicious hosts are not contacted.

Ransomware execution

Post-incident activities for ransomware execution include all the activities involved with malicious code execution, with the addition of ensuring the functionality of a robust offline backup solution. An offline backup solution ensures that backup data is kept inaccessible to ransomware threats and is available if ransomware is successfully executed. A functional and frequent (such as daily incremental and weekly full) backup process helps ensure that business continuity is maintained in the event of issues and incidents.

Denial of service attack

Denial of service post-incident activities should include a timeline of traffic activities, as well as organizational responses to the attack traffic as well as the timeline of any business impacts and the damage associated with the impacts. Any attack precursors should be investigated and noted, and intelligence implemented to notify personnel and potentially take action as soon as attack traffic is observed. Impacts on affected systems should be noted, and a consensus should be reached on whether the systems should be upgraded or supplemented with load-balancing capabilities.

Social Engineering

Post-incident activities for social engineering incidents should include a timeline that includes all applicable activities, such as points of contact, narratives from the parties involved, CCTV footage (if applicable), system and network log files, and physical access control logging data. If unauthorized access was obtained, the impact of the access should be assessed and mitigating factors should be identified for inclusion to reduce the risk of future incidents (such as multifactor authentication, physical locks, greater CCTV coverage, improved physical access control, etc.). Security awareness training should be imperative if policy was breached, and information or access was given to unauthorized parties.

Phishing

Phishing post-incident activities should also include a timeline of actions taken since the phishing email was received, to include descriptions of the type of phishing campaign observed (malicious code, financial exploitation, credential harvesting, etc.), malicious attachments contained (if any), malicious or suspicious links in the body of emails, as well as narratives from recipients of the email and any potential victims, either self-reported or discovered through email, network, or host-based monitoring. If malicious code was included in the campaign, typical post-incident activities involving malicious code should be considered as well. Training opportunities can often arise from phishing attacks, whether successful or not, that can be valuable in giving employees better situational awareness regarding phishing.

The CJIS Security Policy requires each agency with access to CJI to establish operational incident handling procedures (i.e. a local policy). Gleaning from the requirements in Section 5.3 Incident Response, the local policy may include the following elements:

- Overall incident handling procedures. This section describes and identifies the processes used locally how the agency successfully prepares for, manages, and recovers from an incident. It includes sections on:
 - Preparation
 - Detection and Analysis
 - Containment

- Recovery
 - User response activities
- How the agency performs incident reporting. This section describes the process of notifying internal and external partners when an incident has occurred and how the incident is documented. It includes sections on:
 - Internal and external points of contact
 - Required tracking and reporting documents
 - Escalation procedures
- Incident management procedures. This section describes the agency's approach to a consistent and repeatable approach to managing incidents. It includes sections on:
 - Roles and responsibilities
 - Incident-related information collection
 - Updating policies with lessons learned
 - Collection of evidence
 - Incident response training
 - Document and artifact retention

G.8 Secure Coding

Secure Coding

This appendix documents a source of information on best practices and standards for secure coding. With the increased use of software products and the rapid pace of modern software development, it is essential to discover and resolve insecure software risks. The mitigations and guidelines to reduce these common risks can be found in secure coding best practices.

Understanding how software applications work can be a daunting thing; however, it could be key to know if data security is in jeopardy. Awareness of secure coding practices allows an agency to review potential vendors and their products prior to purchase and implementation. It also empowers the agency with the knowledge of the questions to ask a vendor of how the software was developed and whether the vendor uses secure coding practices or standards.

Additionally, the information in this appendix can provide a path forward for agencies with the internal capability to produce “in-house” software applications. By implementing security during the code writing process, security is “baked in” and there is more trust the software will aid in protecting the information it processes.

Open Web Application Security Project (OWASP) Foundation

The OWASP Foundation is a not-for-profit charitable organization focused on improving the security of software. OWASP operates as a community of like-minded professionals to provide unbiased and practical information about application security (AppSec) through software tools and documentation. These materials are available under a free and open software license, which can be located at the link below.

https://www.owasp.org/index.php/Main_Page

Software is becoming increasingly complex and connected, and the difficulty of achieving application security increases exponentially. The rapid pace of modern software development processes makes the most common risks essential to discover and resolve quickly and accurately.

The OWASP Foundation publishes the Top 10 Application Security Risks, which focus on the most serious web application security risks. The OWASP Top 10 is based primarily on 40 plus data submissions from firms that specialize in application security and an industry survey that was completed by over 500 individuals. This data spans vulnerabilities gathered from hundreds of organizations and over 100,000 real world applications and application program interfaces (API). The Top 10 items are selected and prioritized according to this data, in combination with consensus estimates of exploitability, detectability, and impact.

A primary aim of the OWASP Top 10 is to educate developers, designers, architects, managers, and organizations about the consequences of the most common and most important web application security weaknesses. The Top 10 provides basic techniques to protect against these high risks problem areas, and provides guidance on a path forward.

The OWASP Top 10 focuses on identifying the most serious web application security risks for a broad array of organizations. For each of these risks, generic information about likelihood and technical impact using the following simple ratings scheme, which is based on the OWASP Risk Rating Methodology.

Figure G.8-A

The infographic is titled "OWASP Top 10 Application Security Risks – 2017" and is labeled "T10" in a purple box on the left and "6" in a small box on the right. It lists ten security risks, each with a description. The risks are: A1:2017-Injection, A2:2017-Broken Authentication, A3:2017-Sensitive Data Exposure, A4:2017-XML External Entities (XXE), A5:2017-Broken Access Control, A6:2017-Security Misconfiguration, A7:2017-Cross-Site Scripting (XSS), A8:2017-Insecure Deserialization, A9:2017-Using Components with Known Vulnerabilities, and A10:2017-Insufficient Logging & Monitoring.

Risk ID	Risk Name	Description
A1:2017-	Injection	Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
A2:2017-	Broken Authentication	Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.
A3:2017-	Sensitive Data Exposure	Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.
A4:2017-	XML External Entities (XXE)	Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.
A5:2017-	Broken Access Control	Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.
A6:2017-	Security Misconfiguration	Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched and upgraded in a timely fashion.
A7:2017-	Cross-Site Scripting (XSS)	XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
A8:2017-	Insecure Deserialization	Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.
A9:2017-	Using Components with Known Vulnerabilities	Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.
A10:2017-	Insufficient Logging & Monitoring	Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

Each organization is unique, and so are the threat actors for that organization, their goals, and the impact of any breach. It is critical to understand the risk to your organization based on applicable threat agents and business impacts.

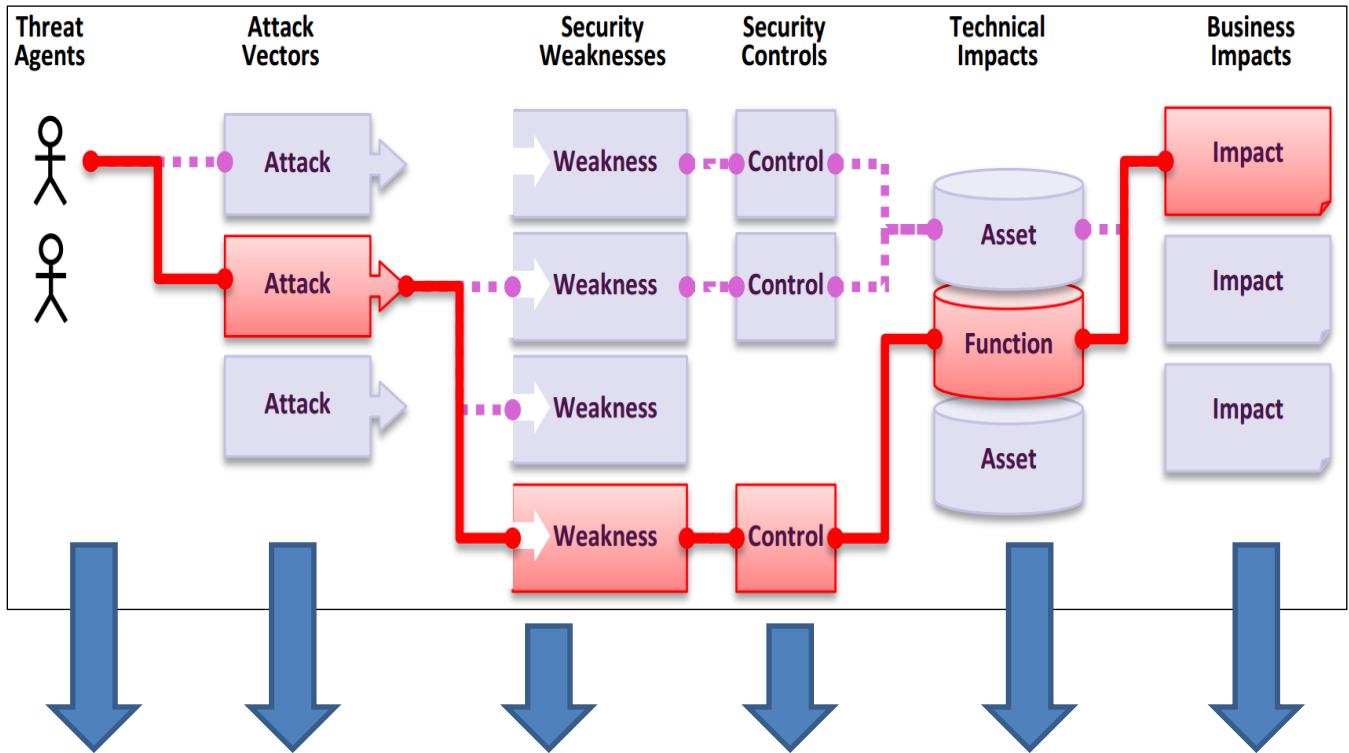
Application Security Risks

The figures immediately below illustrate the path of a sample threat beginning with the threat agent and ending with the target or affected business resource. Various paths are available but the agent would normally select the path of least resistance which would be the most vulnerable and with the fewest number of effective security controls.

The sample risk matrix can be used to assign in the various aspects of potential vulnerability. Each column corresponds to a phase in the attack process. In the matrix, a lower value represents less risk and is more desirable.

Concerning secure coding practices, when security is built-in during code development, vulnerabilities can be identified and controls included reducing the overall risk to information processed by the code.

Figure G.8-B Sample Threat Path



Threat Agents	Exploitability	Weakness Prevalence	Weakness Detectability	Technical Impacts	Business Impacts
App Specific	EASY: 3	WIDESPREAD: 3	EASY: 3	SEVERE: 3	App / Business Specific
	AVERAGE: 2	COMMON: 2	AVERAGE: 2	MODERATE: 2	
	DIFFICULT: 1	UNCOMMON: 1	DIFFICULT: 1	MINOR: 1	

Figure G.8-C General Risk Matrix

To understand these risks for a particular application or organization, you must consider your own specific threat agents and business impacts. Even severe software weaknesses may not present a serious risk if there are no threat agents in a position to perform the necessary attack or the business impact is negligible for the assets involved. The following table presents a summary of the 2017 Top 10 Application Security Risks, and the risk factors that have been assigned to each risk.

Figure G.8-D Top 10 Risk Factor Summary

RISK	Attack Vectors		Security Weakness		Impacts		Score
	Threat Agents	Exploitability	Prevalence	Detectability	Technical	Business	
A1:2017-Injection	App Specific	EASY: 3	COMMON: 2	EASY: 3	SEVERE: 3	App Specific	8.0
A2:2017-Authentication	App Specific	EASY: 3	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	7.0
A3:2017-Sens. Data Exposure	App Specific	AVERAGE: 2	WIDESPREAD: 3	AVERAGE: 2	SEVERE: 3	App Specific	7.0
A4:2017-XML External Entities (XXE)	App Specific	AVERAGE: 2	COMMON: 2	EASY: 3	SEVERE: 3	App Specific	7.0
A5:2017-Broken Access Control	App Specific	AVERAGE: 2	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	6.0
A6:2017-Security Misconfiguration	App Specific	EASY: 3	WIDESPREAD: 3	EASY: 3	MODERATE: 2	App Specific	6.0
A7:2017-Cross-Site Scripting (XSS)	App Specific	EASY: 3	WIDESPREAD: 3	EASY: 3	MODERATE: 2	App Specific	6.0
A8:2017-Insecure Deserialization	App Specific	DIFFICULT: 1	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	5.0
A9:2017-Vulnerable Components	App Specific	AVERAGE: 2	WIDESPREAD: 3	AVERAGE: 2	MODERATE: 2	App Specific	4.7
A10:2017-Insufficient Logging&Monitoring	App Specific	AVERAGE: 2	WIDESPREAD: 3	DIFFICULT: 1	MODERATE: 2	App Specific	4.0

Whether you are new to web application security or already very familiar with these risks, the task of producing a secure web application or fixing an existing one can be difficult. If you have to manage a large application portfolio, this task can be daunting.

To help organizations, developers, testers and managers reduce their application security risks in a cost-effective manner; OWASP has produced numerous free and open resources that you can use to address application security in your organization. The following are some of the many resources OWASP has produced to help organizations produce secure web applications and APIs.

Get Started:

- Document all applications and associated data assets.
- Larger organizations should consider implementing a Configuration Management Database (CMDB).
- Establish an application security program to conduct analysis to define key improvement areas and an execution plan.

Risk Based Portfolio Approach:

- Identify the protection needs of your application portfolio from a business perspective.
- Establish a common risk-rating model with a consistent set of likelihood and impact factors reflective of your organization's tolerance for risk.
- Measure and prioritize all applications and APIs and add results to CMDB.

Enable with a Strong Foundation:

- Establish a set of policies and standards that provide an application security baseline for all development teams to adhere to.
- Define a common set of reusable security controls that complement these policies and standards and provide design and development guidance on their use.

Integrate Security into Existing Processes:

- Define and integrate secure implementation and verification activities into existing development and operational processes.
 - Activities include threat modeling, secure design and design review, secure coding and code review, penetration testing, and remediation.

Application Security Requirements - to produce a secure web application, you must define what secure means for that application.

- [Application Security Verification Standard \(ASVS\):](https://www.owasp.org/index.php/ASVS)
<https://www.owasp.org/index.php/ASVS>
- [OWASP Secure Software Contract Annex:](https://www.owasp.org/index.php/OWASP_Secure_Software_Contract_Annex)
https://www.owasp.org/index.php/OWASP_Secure_Software_Contract_Annex

Application Security Architecture - retrofitting security into your applications and APIs, it is far more cost effective to design the security in from the start.

- OWASP Prevention Cheat Sheets:

https://www.owasp.org/index.php/OWASP_Cheat_Sheet_Series

Standard Security Controls - building strong and usable security controls is difficult. Using a set of standard security controls radically simplifies the development of secure applications and APIs.

- OWASP Proactive Controls:
https://www.owasp.org/index.php/OWASP_Proactive_Controls

Secure Development Lifecycle - to improve the process your organization follows when building applications and APIs, organizations formulate and implement a strategy for software security that is tailored to the specific risks facing their organization.

- OWASP Software Assurance Maturity Model (SAMM):
https://www.owasp.org/index.php/OWASP_SAMM_Project
- OWASP Application Security Guide for CISOs:
https://www.owasp.org/index.php/Application_Security_Guide_For_CISOs

Application Security Education – hands-on learning about vulnerabilities to help educate developers on web application security.

- OWASP Education Project:
https://www.owasp.org/index.php/Category:OWASP_Education_Project
- OWASP WebGoat:
<https://www.owasp.org/index.php/WebGoat>
- OWASP Broken Web Application Project:
https://www.owasp.org/index.php/OWASP_Broken_Web_Applications_Project

Understand the Threat Model – be sure to understand the priorities when it comes to threat model.

- OWASP Testing Guide:
https://www.owasp.org/index.php/OWASP_Testing_Project
- [Application Security Verification Standard \(ASVS\):](https://www.owasp.org/index.php/ASVS)
<https://www.owasp.org/index.php/ASVS>

Testing Strategies – choose the simplest, fastest, most accurate technique to verify each requirement.

- OWASP Security Knowledge Framework:
https://www.owasp.org/index.php/OWASP_Security_Knowledge_Framework

- [Application Security Verification Standard \(ASVS\):
https://www.owasp.org/index.php/ASVS](https://www.owasp.org/index.php/ASVS)

APPENDIX H SECURITY ADDENDUM

The following pages contain:

The legal authority, purpose, and genesis of the Criminal Justice Information Services Security Addendum (H2-H4);

An example of a contract addendum (H-5);

The Security Addendum itself (H6-H7);

The Security Addendum Certification page (H8).

**FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM**

**Legal Authority for and Purpose and Genesis of the
Security Addendum**

Traditionally, law enforcement and other criminal justice agencies have been responsible for the confidentiality of their information. Accordingly, until mid-1999, the Code of Federal Regulations Title 28, Part 20, subpart C, and the National Crime Information Center (NCIC) policy paper approved December 6, 1982, required that the management and exchange of criminal justice information be performed by a criminal justice agency or, in certain circumstances, by a noncriminal justice agency under the management control of a criminal justice agency.

In light of the increasing desire of governmental agencies to contract with private entities to perform administration of criminal justice functions, the FBI sought and obtained approval from the United States Department of Justice (DOJ) to permit such privatization of traditional law enforcement functions under certain controlled circumstances. In the Federal Register of May 10, 1999, the FBI published a Notice of Proposed Rulemaking, announcing as follows:

1. Access to CHRI [Criminal History Record Information] and Related Information, Subject to Appropriate Controls, by a Private Contractor Pursuant to a Specific Agreement with an Authorized Governmental Agency To Perform an Administration of Criminal Justice Function (Privatization). Section 534 of title 28 of the United States Code authorizes the Attorney General to exchange identification, criminal identification, crime, and other records for the official use of authorized officials of the federal government, the states, cities, and penal and other institutions. This statute also provides, however, that such exchanges are subject to cancellation if dissemination is made outside the receiving departments or related agencies. Agencies authorized access to CHRI traditionally have been hesitant to disclose that information, even in furtherance of authorized criminal justice functions, to anyone other than actual agency employees lest such disclosure be viewed as unauthorized. In recent years, however, governmental agencies seeking greater efficiency and economy have become increasingly interested in obtaining support services for the administration of criminal justice from the private sector. With the concurrence of the FBI's Criminal Justice Information Services (CJIS) Advisory Policy Board, the DOJ has concluded that disclosures to private persons and entities providing support services for criminal justice agencies may, when subject to appropriate controls, properly be viewed as permissible disclosures for purposes of compliance with 28 U.S.C. 534.

We are therefore proposing to revise 28 CFR 20.33(a)(7) to provide express authority for such arrangements. The proposed authority is similar to the authority that already exists in 28 CFR 20.21(b)(3) for state and local CHRI systems. Provision of CHRI under this authority would only be permitted pursuant to a specific agreement with an authorized governmental agency for the purpose of providing services for the administration of criminal justice. The agreement would be required to incorporate a security addendum approved by the Director of the FBI (acting for the Attorney General). The security

addendum would specifically authorize access to CHRI, limit the use of the information to the specific purposes for which it is being provided, ensure the security and confidentiality of the information consistent with applicable laws and regulations, provide for sanctions, and contain such other provisions as the Director of the FBI (acting for the Attorney General) may require. The security addendum, buttressed by ongoing audit programs of both the FBI and the sponsoring governmental agency, will provide an appropriate balance between the benefits of privatization, protection of individual privacy interests, and preservation of the security of the FBI's CHRI systems.

The FBI will develop a security addendum to be made available to interested governmental agencies. We anticipate that the security addendum will include physical and personnel security constraints historically required by NCIC security practices and other programmatic requirements, together with personal integrity and electronic security provisions comparable to those in NCIC User Agreements between the FBI and criminal justice agencies, and in existing Management Control Agreements between criminal justice agencies and noncriminal justice governmental entities. The security addendum will make clear that access to CHRI will be limited to those officers and employees of the private contractor or its subcontractor who require the information to properly perform services for the sponsoring governmental agency, and that the service provider may not access, modify, use, or disseminate such information for inconsistent or unauthorized purposes.

Consistent with such intent, Title 28 of the Code of Federal Regulations (C.F.R.) was amended to read:

§ 20.33 Dissemination of criminal history record information.

- a) Criminal history record information contained in the Interstate Identification Index (III) System and the Fingerprint Identification Records System (FIRS) may be made available:
 - 1) To criminal justice agencies for criminal justice purposes, which purposes include the screening of employees or applicants for employment hired by criminal justice agencies.
 - 2) To noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing/information services for criminal justice agencies; and
 - 3) To private contractors pursuant to a specific agreement with an agency identified in paragraphs (a)(1) or (a)(6) of this section and for the purpose of providing services for the administration of criminal justice pursuant to that agreement. The agreement must incorporate a security addendum approved by the Attorney General of the United States, which shall specifically authorize access to criminal history record information, limit the use of the information to the purposes for which it is provided, ensure the security and confidentiality of the information consistent with these regulations, provide for sanctions, and contain such other provisions as the Attorney General may require. The power

and authority of the Attorney General hereunder shall be exercised by the FBI Director (or the Director's designee).

This Security Addendum, appended to and incorporated by reference in a government-private sector contract entered into for such purpose, is intended to insure that the benefits of privatization are not attained with any accompanying degradation in the security of the national system of criminal records accessed by the contracting private party. This Security Addendum addresses both concerns for personal integrity and electronic security which have been addressed in previously executed user agreements and management control agreements.

A government agency may privatize functions traditionally performed by criminal justice agencies (or noncriminal justice agencies acting under a management control agreement), subject to the terms of this Security Addendum. If privatized, access by a private contractor's personnel to NCIC data and other CJIS information is restricted to only that necessary to perform the privatized tasks consistent with the government agency's function and the focus of the contract. If privatized the contractor may not access, modify, use or disseminate such data in any manner not expressly authorized by the government agency in consultation with the FBI.

EXAMPLE OF A CONTRACT ADDENDUM

AMENDMENT NO. ____ TO THE CONTRACT BETWEEN
[PARTY NO. 1] AND [PARTY NO. 2], ENTERED INTO [DATE]

[Name of Law Enforcement Agency] and [Party No. 2], upon notification and pursuant to Paragraph/Section No. ____ [the amendment clause of the original contract] of that certain contract entered into by these parties on [date][and entitled "____"], hereby amend and revise the contract to include the following:

1. Access to and use of criminal history record information and other sensitive information maintained in [state and] FBI-managed criminal justice information systems by [private party] are subject to the following restrictions:

- a.
- b.
- c.

and

d. The Security Addendum appended hereto, which is incorporated by reference and made a part thereof as if fully appearing herein.

This amendment is effective the ____ day of _____, 20__.

On behalf of [Party No. 1]: _____

[Name]

[Title]

Date

On behalf of [Party No. 2]: _____

[Name]

[Title]

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A-130 as “security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.”

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

1.00 Definitions

1.01 Contracting Government Agency (CGA) - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.02 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.00 Responsibilities of the Contracting Government Agency.

2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

3.00 Responsibilities of the Contractor.

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.00 Security Violations.

4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

- a. Investigate or decline to investigate any report of unauthorized use;
- b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:

Information Security Officer

Criminal Justice Information Services Division, FBI

1000 Custer Hollow Road

Clarksburg, West Virginia 26306

**FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM**

CERTIFICATION

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

Printed Name/Signature of Contractor Employee

Date

Printed Name/Signature of Contractor Representative

Date

Organization and Title of Contractor Representative

APPENDIX I REFERENCES

- White House Memo entitled “Designation and Sharing of Controlled Unclassified Information (CUI)”, May 9, 2008
- [CJIS RA] *CJIS Security Policy Risk Assessment Report*; August 2008; For Official Use Only; Prepared by: Noblis; Prepared for: U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division, 1000 Custer Hollow Road, Clarksburg, WV 26306
- [CNSS Instruction No. 4009] *National Information Assurance (IA) Glossary*; Committee on National Security Systems (CNSS) Instruction No. 4009; 26 April 2010
- [FBI SA 8/2006] *Federal Bureau of Investigation, Criminal Justice Information Services, Security Addendum*; 8/2006; Assistant Director, Criminal Justice Information Services, FBI, 1000 Custer Hollow Road, Clarksburg, West Virginia 26306
- [FISMA] *Federal Information Security Management Act of 2002*; House of Representatives Bill 2458, Title III–Information Security
- [FIPS 199] *Standards for Security Categorization of Federal Information and Information Systems*; Federal Information Processing Standards Publication, FIPS PUB 199; February 2004
- [FIPS 200] *Minimum Security Requirements for Federal Information and Information Systems*; Federal Information Processing Standards Publication, FIPS PUB 200; March 2006
- [FIPS 201] *Personal Identity Verification for Federal Employees and Contractors*; Federal Information Processing Standards Publication, FIPS PUB 201-1
- [NIST SP 800–14] *Generally Accepted Principles and Practices for Securing Information Technology Systems*; NIST Special Publication 800–14
- [NIST SP 800–25] *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*; NIST Special Publication 800–25
- [NIST SP 800–30] *Risk Management Guide for Information Technology Systems*; NIST Special Publication 800–36
- [NIST SP 800–32] *Introduction to Public Key Technology and the Federal PKI Infrastructure*; NIST Special Publication 800–32
- [NIST SP 800–34] *Contingency Planning Guide for Information Technology Systems*; NIST Special Publication 800–34
- [NIST SP 800–35] *Guide to Information Technology Security Services*; NIST Special Publication 800–35
- [NIST SP 800–36] *Guide to Selecting Information Technology Security Products*; NIST Special Publication 800–36
- [NIST SP 800–39] *Managing Risk from Information Systems, An Organizational Perspective*; NIST Special Publication 800–39
- [NIST SP 800–40] *Procedures for Handling Security Patches*; NIST Special Publication 800–40

- [NIST SP 800–44] *Guidelines on Securing Public Web Servers*; NIST Special Publication 800–44
- [NIST SP 800–45] *Guidelines on Electronic Mail Security*; NIST Special Publication 800–45, Version 2
- [NIST SP 800–46] *Security for Telecommuting and Broadband Communications*; NIST Special Publication 800–46
- [NIST SP 800–48] *Wireless Network Security: 802.11, Bluetooth, and Handheld Devices*; NIST Special Publication 800–48
- [NIST SP 800–52] *Guidelines on the Selection and Use of Transport Layer Security*; NIST Special Publication 800–52
- [NIST SP 800–53] *Recommended Security Controls for Federal Information Systems*; NIST Special Publication 800–53, Revision 2
- [NIST SP 800–53A] *Guide for Assessing the Security Controls in Federal Information Systems, Building Effective Security Assessment Plans*; NIST Special Publication 800–53A
- [NIST SP 800–58] *Security Considerations for Voice over IP Systems*; NIST Special Publication 800–58
- [NIST SP 800–60] *Guide for Mapping Types of Information and Information Systems to Security Categories*; NIST Special Publication 800–60, Revision 1, DRAFT
- [NIST SP 800–63–1] *Electronic Authentication Guideline*; NIST Special Publication 800–63–1; DRAFT
- [NIST SP 800–64] NIST Special Publication 800–64
- [NIST SP 800–66] *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA)*; NIST Special Publication 800–66
- [NIST SP 800–68] *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*; NIST Special Publication 800–68
- [NIST SP 800–70] *Security Configuration Checklists Program for IT Products*; NIST Special Publication 800–70
- [NIST SP 800–72] *Guidelines on PDA Forensics*; NIST Special Publication 800–72
- [NIST SP 800–73] *Integrated Circuit Card for Personal Identification Verification*; NIST Special Publication 800–73; Revision 1
- [NIST SP 800–76] *Biometric Data Specification for Personal Identity Verification*; NIST Special Publication 800–76
- [NIST SP 800–77] *Guide to IPSec VPNs*; NIST Special Publication 800–77
- [NIST SP 800–78] *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*; NIST Special Publication 800–78
- [NIST SP 800–81] *Secure Domain Name System (DNS) Deployment Guide*; NIST Special Publication 800–81
- [NIST SP 800–84] *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*; NIST Special Publication 800–84

- [NIST SP 800–86] *Guide to Integrating Forensic Techniques into Incident Response*; NIST Special Publication 800–86
- [NIST SP 800–87] *Codes for the Identification of Federal and Federally Assisted Agencies*; NIST Special Publication 800–87
- [NIST SP 800–96] *PIV Card / Reader Interoperability Guidelines*; NIST Special Publication 800–96
- [NIST SP 800–97] *Guide to IEEE 802.11i: Robust Security Networks*; NIST Special Publication 800–97
- [NIST SP 800–121] *Guide to Bluetooth Security*, NIST Special Publication 800-121
- [NIST SP 800–124] *Guidelines on Cell Phone and PDA Security*, NIST Special Publication 800-124
- [NIST SP 800-125] *Guide to Security for Full Virtualization Technologies*; NIST Special Publication 800-125
- [NIST SP 800–144] *Guidelines on Security and Privacy in Public Cloud Computing*; NIST Special Publication 800-144
- [NIST SP 800–145] *The NIST Definition of Cloud Computing*; NIST Special Publication 800-145
- [NIST SP 800–146] *Cloud Computing Synopsis and Recommendations*; NIST Special Publication 800-146
- [OMB A–130] *Management of Federal Information Resources*; Circular No. A–130; Revised; February 8, 1996
- [OMB M–04–04] *E-Authentication Guidance for Federal Agencies*; OMB Memo 04–04; December 16, 2003
- [OMB M–06–15] *Safeguarding Personally Identifiable Information*; OMB Memo 06–15; May 22, 2006
- [OMB M–06–16] *Protection of Sensitive Agency Information*; OMB Memo 06–16; June 23, 2006
- [OMB M–06–19] *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*; OMB Memo 06–19; July 12, 2006
- [OMB M–07–16] *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*; OMB Meme 07–16; May 22, 2007
- [Surviving Security] *Surviving Security: How to Integrate People, Process, and Technology*; Second Edition; 2004
- [USC Title 5, Section 552] *Public information; agency rules, opinions, orders, records, and proceedings*; United States Code, Title 5 - Government Agency and Employees, Part I - The Agencies Generally, Chapter 5 - Administrative Procedure, Subchapter II - Administrative Procedure, Section 552. Public information; agency rules, opinions, orders, records, and proceedings

[USC Title 44, Section 3506] *Federal Information Policy*; 01/02/2006; United States Code,
Title 44 - Public Printing and Documents; Chapter 35 - Coordination of
Federal Information Policy; Subchapter I - Federal Information Policy, Section
3506

APPENDIX J NONCRIMINAL JUSTICE AGENCY SUPPLEMENTAL GUIDANCE

This appendix is not intended to be used in lieu of the CJIS Security Policy (CSP) but rather should be used as supplemental guidance specifically for those Noncriminal Justice Agencies (NCJA) with access to Criminal Justice Information (CJI) as authorized by legislative enactment or federal executive order to request civil fingerprint-based background checks for licensing, employment, or other noncriminal justice purposes, via their State Identification Bureau (SIB) and/or Channeling agency. Examples of the target audience for the Appendix J supplemental guidance include school boards, banks, medical boards, gaming commissions, alcohol and tobacco control boards, social services agencies, pharmacy boards, etc.

The CSP is the minimum standard policy used by both criminal and noncriminal justice agencies requiring access to CJI maintained by the FBI CJIS Division. The essential premise of the CSP is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CSP provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information.

For those NCJAs new to the CSP and Advisory Policy Board (APB) auditing process (all NCJAs will be periodically audited by the CJIS Systems Agency (CSA)/SIB and may be included in a sampling of triennial audits conducted by the FBI) it is strongly recommended that each system processing CJI should be individually reviewed to determine which CSP requirements may apply. In the interim however this supplemental guidance provides a minimum starting point that every NCJA processing CJI can immediately put into place. Once the broader array of security controls are gleaned for a specific system, agencies can then leverage the (already implemented) controls described in this appendix as a launching pad towards full policy compliance.

The following information is organized to provide the section and section title within the CSP, along with a brief summary and background on the guidance itself. For the specific “shall” statement please go to the referenced section within the main body of the CSP.

General CJI Guidance

The following information provides NCJAs guidance to maintain security compliance when setting up any system capable of sending and/or receiving CJI:

a. **3.2.9 – Local Agency Security Officer (LASO)**

It is the responsibility of the CJIS Systems Officer (CSO) to ensure each agency having access to CJI has someone designated as the Local Agency Security Officer (LASO) per CSP Section 3.2.2(2e).

The LASO serves as the primary point of contact (POC) between the local NCJA and their respective CSA CSO or Information Security Officer (ISO) who interfaces with the FBI CJIS Division. The LASO actively represents their agency in all matters pertaining to information security, disseminates information security alerts and other material to their constituents, maintains information security documentation (including system configuration data), assists with Information Security audits of hardware and

procedures, and keeps the CSA (i.e., CSO or ISO) informed as to any information security needs and problems.

b. 5.1.1.6 – Agency User Agreements

When an NCJA (private or public) is permitted to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions as authorized pursuant to federal law or state statute approved by the U.S. Attorney General, the information received from the background check, such as criminal history record information (CHRI) or personally identifiable information (PII), must be protected as CJI. In order to receive access to CJI the NCJA must enter into a signed written agreement, i.e., an agency user agreement, with the appropriate signatory authority of the CSA, SIB, or authorized agency providing the CJI access. An example of a NCJA (private) is a local bank. An example of a NCJA (public) is a county school board.

Note 1: The CSA, SIB, or authorized agency providing the CJI access term should be part of the agency user agreement.

Note 2: Any NCJA that directly accesses FBI CJIS must allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system.

c. 5.1.3 – Secondary Dissemination

Secondary dissemination is the promulgation of CJI from a releasing agency to an authorized recipient agency that has not been previously identified in a formal information exchange agreement.

If CHRI is released to another authorized agency, that is not part of the releasing agency's primary information exchange agreement(s), the releasing agency must log such dissemination.

d. 5.2.1.1 – All Personnel (Security Awareness Training)

Basic security awareness training is required for all personnel who have access to CJI within six months of initial assignment, and biennially thereafter. CSP Section 5.2.1.1 describes the topics that must be addressed within baseline security awareness training for all authorized personnel with access to CJI.

Note: The CSO/SIB may accept the documentation of the completion of security awareness training from another agency. Accepting such documentation from another agency means that the accepting agency assumes the risk that the training may not meet a particular requirement or process required by federal, state, or local laws.

e. 5.3 – Incident Response

CSP Section 5.3 assists agencies with response and reporting procedures for accidental and malicious computer and network attacks. The requirements within Section 5.3 will help NCJAs with:

- (i) Establishing an operational incident handling capability for agency information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and,
- (ii) Tracking, documenting, and reporting incidents to appropriate agency officials and/or authorities.

CSP Section 5.3.1 describes the requirements for reporting security events and describes the responsibilities of the FBI CJIS Division and the CSA ISO.

CSP Section 5.3.2 describes the requirements for managing security incidents, to include: incident handling and the collection of evidence.

CSP Section 5.3.3 describes the requirement for an agency to ensure general incident response roles responsibilities are included as part of required security awareness training.

CSP Section 5.3.4 describes the requirement for an agency to track and document information system security incidents on an ongoing basis.

Note 1: CSA ISOs serve as the POC on security-related issues for their respective agencies and must ensure LASOs institute the CSA incident response reporting procedures at the local level. The CSA ISO shall maintain completed security incident reporting forms until the subsequent FBI triennial audit or until legal action (if warranted) is complete; whichever time-frame is greater.

Note 2: CSP Appendix F contains a sample incident notification letter for use when communicating the details of an incident to the FBI CJIS ISO.

f. 5.4 – Auditing and Accountability

CSP Section 5.4 assists agencies in assessing the inventory of components that compose their information systems to determine which security controls are applicable to the various components and implement required audit and accountability controls.

CSP Section 5.4.1 describes the required parameters for agencies to generate audit records and content for defined events and periodically review and update the list of agency-defined auditable events.

CSP Section 5.4.2 describes the requirement for agencies to provide alerts to appropriate agency officials in the event of an audit processing failure, such as software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

CSP Section 5.4.3 describes the requirements for audit review/analysis frequency and to designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions.

CSP Section 5.4.4 describes the requirement to establish information system time stamp parameters for use in audit record generation.

CSP Section 5.4.5 describes the requirement to protect audit information and audit tools from modification, deletion and unauthorized access.

CSP Section 5.4.6 describes the requirement for an agency to retain audit records for at least one (1) year.

Note: The agency will continue to retain audit records for longer than one (1) year until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes - for example, retention and availability of audit records relative

to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions.

CSP Section 5.4.7 describes the requirements for logging National Crime Information Center (NCIC) and Interstate Identification Index (III) transactions. A log must be maintained for a minimum of one (1) year on all NCIC and III transactions. The III portion of the log will clearly identify both the operator and the authorized receiving agency. III logs must also clearly identify the requester and the secondary recipient. The identification on the log will take the form of a unique identifier that shall remain unique to the individual requester and to the secondary recipient throughout the minimum one (1) year retention period.

g. 5.8 – Media Protection

CJIS Security Policy Section 5.8 assists agencies to document and implement media protection policy and procedures required to ensure that access to electronic and physical media in all forms is restricted to authorized individuals for securely handling, transporting and storing media.

“Electronic media” is electronic storage media, such as memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card. “Physical media” refers to CJIS in physical form, e.g. printed documents, printed imagery, etc.

CSP Section 5.8.1 describes the requirement for agencies to securely store electronic and physical media within physically secure locations or controlled areas and restrict access to electronic and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data must be encrypted per CSP Section 5.10.1.2.

CSP Section 5.8.2 describes the requirements for agencies to protect and control both electronic and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel. The agency is responsible for implementing controls to protect electronic media containing CJIS while in transport (physically moved from one location to another) to help prevent compromise of the data. Encryption, as defined in CSP Section 5.10.1.2, is the optimal control; however, if encryption of the data isn’t possible then each agency must institute other controls to ensure the security of the data.

CSP Section 5.8.3 describes the requirements for agencies to maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies must sanitize (electronically overwrite the data at least three times) or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. This sanitization or destruction needs to be witnessed or carried out only by authorized personnel. Inoperable electronic media must be destroyed (cut up, shredded, etc.).

CSP Section 5.8.4 describes the requirements for physical media to be securely disposed of when no longer required, using established formal procedures. Physical media must be destroyed by shredding or incineration. This disposal or destruction needs to be witnessed or carried out only by authorized personnel.

h. 5.9 Physical Protection

CSP Section 5.9 explains the physical protection policy and procedures that are required to ensure CJI and information system hardware, software, and media are physically protected through access control measures.

CSP Section 5.9.1 details the requirements for establishing a Physically Secure Location - a facility, a criminal justice conveyance, an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems. Sections 5.9.1.1 – 5.9.1.8 describe the physical control requirements that must be implemented in order to establish a physically secure location.

CSP Section 5.9.2 details the requirements for establishing a Controlled Area. The controlled area is an area, a room, or a storage container established for the purpose of day-to-day CJI access, storage, or processing in the event an agency is unable to meet all of the controls required for establishing a physically secure location. Access to the controlled area needs to be restricted to only authorized personnel whenever CJI is processed. The CJI material needs to be locked away when unattended to prevent unauthorized and unintentional access. Additionally, the encryption standards of CSP Section 5.10.1.2 apply to the electronic storage (i.e. data “at rest”) of CJI.

i. 5.11 – Formal Audits

CSP Section 5.11 explains the formal audit process to help agencies understand the audit procedures.

CSP Section 5.11.1 details the requirements for compliance and security audits by the FBI CJIS Division. The FBI CJIS Division is authorized to conduct audits, once every three (3) years as a minimum, to assess agency compliance with applicable statutes, regulations and policies.

The CJIS Audit Unit (CAU) will conduct triennial audits of each CSA in order to verify compliance with applicable statutes, regulations and policies. This audit includes a sample of Criminal Justice Agency (CJA) and NCJAs, in coordination with the SIB.

Note 1: Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with applicable statutes, regulations and policies.

Note 2: The FBI CJIS Division has the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

CSP Section 5.11.2 describes the requirements for the CSA to triennially audit all CJAs and NCJAs with direct access to the state system, establish a process to periodically audit all NCJAs with access to CJI, establish the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

CSP Section 5.11.3 describes the requirement that all agencies with access to CJI must permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations. The inspection team, appointed by the APB, will include at least one representative of the CJIS Division. All results of the inquiry and audit will be reported to the APB with appropriate recommendations.

Agencies located within states having passed legislation authorizing or requiring civil fingerprint-based background checks for personnel with access to criminal history record

information for the purposes of licensing or employment need to follow the guidance in Section 5.12 (referenced below).

j. 5.12 – Personnel Security

CSP Section 5.12 provides agencies the security terms and requirements as they apply to all personnel who have unescorted access to unencrypted CJI, including individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI.

CSP Section 5.12.1 details the minimum screening requirements for all individuals requiring unescorted access to unencrypted CJI.

CSP Section 5.12.2 describes the requirement for an agency to immediately terminate CJI access for an individual upon termination of employment.

CSP Section 5.12.3 describes the requirement for an agency to review CJI access authorizations and initiate appropriate actions (such as closing and establishing accounts and changing system access authorizations) whenever personnel are reassigned or transferred to other positions within the agency.

CSP Section 5.12.4 describes the requirement for an agency to employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.

Agencies located within states that have not passed legislation authorizing or requiring civil fingerprint-based background checks are exempted from this requirement until such time as appropriate legislation has been written into law.

The following scenarios are intended to help the reader identify areas within the CSP that NCJAs may often come across. Each scenario should be reviewed for applicability in conjunction with the above General CJI Guidance section. The specific requirements found with the CSP are not shown; however specific sections are referenced along with a requirements summary.

Hard Copy CJI Storage and Accessibility

When an NCJA receives CJI via a paper copy from a CJA and stores the paper within a locked file cabinet, the NCJA should, in addition to the General CJI Guidance, focus on compliance with policy section:

a. 4.2.4 – Storage

When storing CJI, appropriate administrative, technical, and physical safeguards must be implemented to ensure the security and confidentiality of the information.

Electronic CJI Storage and Accessibility – Controlled Area

When an NCJA creates an electronic copy of CJI (e.g. scanning a document or creation of a spreadsheet) and subsequently stores this static CJI on either a local hard drive or shared network drive in a controlled area for indirect access by Authorized Recipients, the NCJA should, in addition to the General CJI Guidance, focus on compliance with policy section:

a. 5.5.2.4 (3) – Access Control – Encryption

CSP Section 5.5.2.4 item 3 – Encryption describes the requirement for utilizing encryption as the primary access control mechanism which is necessary in this situation. Encrypted information can only be read by personnel possessing the

appropriate cryptographic key (e.g., passphrase) to decrypt. Refer to Section 5.10.1.2 for specific encryption requirements.

Electronic CJI Storage and Accessibility – Physically Secure Location

When an NCJA receives or creates an electronic copy of CJI and subsequently stores this CJI within a Records Management System (RMS), located within a physically secure location that may be queried by Authorized Recipients, the NCJA should, in addition to the General CJI Guidance, focus on compliance with policy sections:

a. **5.5 – Access Control**

CSP Section 5.5 describes the requirements and parameters for utilizing access control mechanisms for restricting CJI access (such as the reading, writing, processing and transmission of CJIS information) and the modification of information systems, applications, services and communication configurations allowing access to CJI to only authorized personnel.

b. **5.6 – Identification and Authentication**

CSP Section 5.6 describes the requirements and parameters agencies must implement to validate and authenticate the identity of information system users and processes acting on behalf of users the identities prior to granting access to CJI or agency information systems/services that process CJI.

c. **5.7 – Configuration Management**

CSP Section 5.7 describes the requirements for implementing access restrictions that will only permit authorized and qualified individuals access to information system components for purposes of initiating changes, including upgrades, and modifications.

CSP Section 5.7.1 describes the requirements for implementing the concept of least privilege (5.7.1.1) and for developing and maintaining network diagrams (5.7.1.2) that detail how the RMS is interconnected and protected within the network. See Appendix C for sample network diagrams.

CSP Section 5.7.2 details the requirement for agencies to protect the system documentation from unauthorized access consistent with the provisions described in Section 5.5 Access Control.

d. **5.10 – System and Communications Protection and Information Integrity**

CSP Section 5.10 details the requirements for network infrastructures within physically secure locations through establishment of system and communication boundary and transmission protection safeguards that assist in securing an agency’s environment, even when virtualized. In addition, this section describes the requirements for providing the capability to ensure system integrity through the detection and protection against unauthorized changes to software and information for applications, services, and information systems.

Use Case Scenarios

1. Indirect Access to Criminal Justice Information (CJI) Stored on a Network Server

A county board of education is converting all employee records, including background check information containing CJI, to an electronic format. The records will be scanned from hard copy to electronic files and placed on network server that has indirect access to CJI and is located in a secure data center within the board of education offices. The data center meets all the requirements to be labeled a physically secure location as defined in Section 5.9.1 of the CSP.

Keeping in mind the scenario as described, an authorized user needs access to an employee's electronic record. This user is not located in the secure data center and will have to use remote access to access the file. The user is therefore required to provide identification and authentication credentials to prove they are an authorized user. To access the record, the user is prompted to enter their unique username and password. Because the record resides on a system with indirect access to CJI (does not allow the user to query a state or national criminal record repository), AA is not required to access the record.

NOTE: If the Authorized User has direct access to CJI (the ability to query a state or national criminal record repository) in the above scenario, AA would be required.

2. Encryption for Data at Rest (Exemption for FIPS 140-2 Certified Encryption)

A county board of education is converting all employee records, including background check information containing CJI, to an electronic format. The records will be scanned from hard copy to electronic files and placed on network server that is not located in a secure data center. Because the data center does not meet the requirements of a physically secure location, as defined in Section 5.9.1 of the CSP, the files, at rest (in storage) on the server, are required to be encrypted.

To prevent unauthorized access, the IT staff has decided to encrypt the entire folder that contains the files. They will use a product that provides an advanced encryption standard (AES) encryption algorithm at 256 bit strength to comply with the CSP and employ a CSP compliant passphrase to lock the folder's encryption. When an authorized user needs to access an employee's record, they access the folder on the server and are prompted to enter the designated passphrase to decrypt (unlock) the folder. The user can then access all files within the folder.

NOTE: Whenever authorized personnel no longer require access to the encrypted folder, the passphrase must be changed to prevent future access by that user.

APPENDIX K CRIMINAL JUSTICE AGENCY SUPPLEMENTAL GUIDANCE

This appendix is not intended to be used in lieu of the CJIS Security Policy (CSP) but rather should be used as supplemental guidance specifically for those Criminal Justice Agencies (CJA) that have historically not been subject to audit under the CJIS Security Policy guidelines. The target audience typically gains access to CJI via fax, hardcopy distribution or voice calls; does not have the capability to query state or national databases for criminal justice information; and may have been assigned an originating agency identifier (ORI) but is dependent on other agencies to run queries on their behalf. This guidance is not intended for criminal justice agencies covered under an active information exchange agreement with another agency for direct or indirect connectivity to the state CJIS Systems Agency (CSA) – in other words those agencies traditionally identified as “terminal agencies”.

The CSP is the minimum standard policy used by both criminal and noncriminal justice agencies requiring access to criminal justice information (CJI) maintained by the FBI CJIS Division. The essential premise of the CSP is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CSP provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information.

For those CJAs new to the CSP it is strongly recommended that each system processing CJI should be individually reviewed to determine which CSP requirements may apply. In the interim however this supplemental guidance provides a minimum starting point that every CJA processing CJI can immediately put into place. Once the broader array of security controls are gleaned for a specific system, agencies can then leverage the (already implemented) controls described in this appendix as a launching pad towards full policy compliance.

The following information is organized to provide the section and section title within the CSP, along with a brief summary and background on the guidance itself. For the specific “shall” statement please go to the referenced section within the main body of the CSP.

General CJI Guidance

The following information provides CJAs guidance to maintain security compliance when setting up any system capable of sending and/or receiving CJI:

a. **3.2.9 – Local Agency Security Officer (LASO)**

It is the responsibility of the CJIS Systems Officer (CSO) to ensure each agency having access to CJI has someone designated as the Local Agency Security Officer (LASO) per CSP Section 3.2.2(2e).

The LASO serves as the primary point of contact (POC) between the local CJA and their respective CSA CSO or Information Security Officer (ISO) who interfaces with the FBI CJIS Division. The LASO actively represents their agency in all matters pertaining to information security, disseminates information security alerts and other material to their constituents, maintains information security documentation (including system configuration data), assists with Information Security audits of hardware and procedures, and keeps the CSA (i.e., CSO or ISO) informed as to any information security needs and problems.

b. 5.1.1.3 – Criminal Justice Agency User Agreements

Any CJA receiving access to CJI must enter into a signed agreement with the CSA providing the access. The agreement specifies the services and systems the agency will access. It must also specify all pertinent governance policies to which the agency must adhere.

c. 5.1.3 – Secondary Dissemination

Secondary dissemination is the promulgation of CJI from a releasing agency to an authorized recipient agency that has not been previously identified in a formal information exchange agreement.

If CHRI is released to another authorized agency, that is not part of the releasing agency's primary information exchange agreement(s), the releasing agency must log such dissemination.

d. 5.2 – Security Awareness Training

Basic security awareness training is required for all personnel who have access to CJI within six months of initial assignment, and biennially thereafter. CSP Section 5.2.1.1 describes the topics that must be addressed within baseline security awareness training for all authorized personnel with access to CJI.

CSP Section 5.2.1.2 describes the topics required to be discussed for personnel that have both physical and logical access to CJI. These topics are covered in addition to the ones addressed in basic security awareness training.

CSP Section 5.2.1.3 describes topics to be covered for those personnel assigned information technology roles. Topics covered in this section are in addition to the topics addressed in Sections 5.2.1.1 and 5.2.1.2.

Note: The CSO may accept the documentation of the completion of security awareness training from another agency. Accepting such documentation from another agency means that the accepting agency assumes the risk that the training may not meet a particular requirement or process required by federal, state, or local laws.

e. 5.3 – Incident Response

CSP Section 5.3 assists agencies with response and reporting procedures for accidental and malicious computer and network attacks. The requirements within Section 5.3 will help CJAs with:

- (iii) Establishing an operational incident handling capability for agency information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and,
- (iv) Tracking, documenting, and reporting incidents to appropriate agency officials and/or authorities.

CSP Section 5.3.1 describes the requirements for reporting security events and describes the responsibilities of the FBI CJIS Division and the CSA ISO.

CSP Section 5.3.2 describes the requirements for managing security incidents, to include: incident handling and the collection of evidence.

CSP Section 5.3.3 describes the requirement for an agency to ensure general incident response roles responsibilities are included as part of required security awareness training.

CSP Section 5.3.4 describes the requirement for an agency to track and document information system security incidents on an ongoing basis.

Note 1: CSA ISOs serve as the POC on security-related issues for their respective agencies and must ensure LASOs institute the CSA incident response reporting procedures at the local level. The CSA ISO shall maintain completed security incident reporting forms until the subsequent FBI triennial audit or until legal action (if warranted) is complete; whichever time-frame is greater.

Note 2: CSP Appendix F contains a sample incident notification letter for use when communicating the details of an incident to the FBI CJIS ISO.

f. 5.4 – Auditing and Accountability

CSP Section 5.4 assists agencies in assessing the inventory of components that compose their information systems to determine which security controls are applicable to the various components and implement required audit and accountability controls.

CSP Section 5.4.1 describes the required parameters for agencies to generate audit records and content for defined events and periodically review and update the list of agency-defined auditable events.

CSP Section 5.4.2 describes the requirement for agencies to provide alerts to appropriate agency officials in the event of an audit processing failure, such as software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

CSP Section 5.4.3 describes the requirements for audit review/analysis frequency and to designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions.

CSP Section 5.4.4 describes the requirement to establish information system time stamp parameters for use in audit record generation.

CSP Section 5.4.5 describes the requirement to protect audit information and audit tools from modification, deletion and unauthorized access.

CSP Section 5.4.6 describes the requirement for an agency to retain audit records for at least one (1) year.

Note: The agency will continue to retain audit records for longer than one (1) year until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes - for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions.

CSP Section 5.4.7 describes the requirements for logging National Crime Information Center (NCIC) and Interstate Identification Index (III) transactions. A log must be maintained for a minimum of one (1) year on all NCIC and III transactions. The III portion of the log will clearly identify both the operator and the authorized receiving agency. III logs must also clearly identify the requester and the secondary recipient.

The identification on the log will take the form of a unique identifier that shall remain unique to the individual requester and to the secondary recipient throughout the minimum one (1) year retention period.

g. 5.8 – Media Protection

CJIS Security Policy Section 5.8 assists agencies to document and implement media protection policy and procedures required to ensure that access to digital and physical media in all forms is restricted to authorized individuals for securely handling, transporting and storing media.

“Digital media” is electronic storage media, such as memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card. “Physical media” refers to CJI in physical form, e.g. printed documents, printed imagery, etc.

CSP Section 5.8.1 describes the requirement for agencies to securely store digital and physical media within physically secure locations or controlled areas and restrict access to electronic and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data must be encrypted per CSP Section 5.10.1.2.

CSP Section 5.8.2 describes the requirements for agencies to protect and control both digital and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel. The agency is responsible for implementing controls to protect electronic media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data. Encryption, as defined in CSP Section 5.10.1.2, is the optimal control; however, if encryption of the data isn’t possible then each agency must institute other controls to ensure the security of the data.

CSP Section 5.8.3 describes the requirements for agencies to maintain written documentation of the steps taken to sanitize or destroy digital media. Agencies must sanitize (electronically overwrite the data at least three times) or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. This sanitization or destruction needs to be witnessed or carried out only by authorized personnel. Inoperable electronic media must be destroyed (cut up, shredded, etc.).

CSP Section 5.8.4 describes the requirements for physical media to be securely disposed of when no longer required, using established formal procedures. Physical media must be destroyed by shredding or incineration. This disposal or destruction needs to be witnessed or carried out only by authorized personnel.

h. 5.9 Physical Protection

CSP Section 5.9 explains the physical protection policy and procedures that are required to ensure CJI and information system hardware, software, and media are physically protected through access control measures.

CSP Section 5.9.1 details the requirements for establishing a Physically Secure Location - a facility, a police vehicle, an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems. Sections 5.9.1.1 – 5.9.1.8 describe the physical control requirements that must be implemented in order to establish a physically secure location.

CSP Section 5.9.2 details the requirements for establishing a Controlled Area. The controlled area is an area, a room, or a storage container established for the purpose of day-to-day CJI access, storage, or processing in the event an agency is unable to meet all of the controls required for establishing a physically secure location. Access to the controlled area needs to be restricted to only authorized personnel whenever CJI is processed. The CJI material needs to be locked away when unattended to prevent unauthorized and unintentional access. Additionally, the encryption standards of CSP Section 5.10.1.2 apply to the electronic storage (i.e. data “at rest”) of CJI.

i. 5.10 – System and Communications Protection and Information Integrity

CSP Section 5.10 explains the technical safeguards ranging from boundary and transmission protection to security an agency’s virtualized environment.

CSP Section 5.10.1.2 details the requirements for the encryption of CJI whether in transit or at rest. FIPS 140-2 certification is required when CJI is in transit outside a physically secure location. When at rest outside a physically secure location, encryption methods can use Advanced Encryption Standard (AES) at 256 bit strength or a FIPS 140-2 certified method.

CSP Section 5.10.3 explains the use of virtualization and partitioning when processing CJI in a virtual environment. A virtualized environment can be configured such that those parts of the system which process CJI are either physically or virtually separated from those that do not.

CSP Section 5.10.4 explains system and information integrity policy and procedures. This includes areas such as patch management, malicious code protection, and spam and spyware protection.

j. 5.11 – Formal Audits

CSP Section 5.11 explains the formal audit process to help agencies understand the audit procedures.

CSP Section 5.11.1 details the requirements for compliance and security audits by the FBI CJIS Division. The FBI CJIS Division is authorized to conduct audits, once every three (3) years as a minimum, to assess agency compliance with applicable statutes, regulations and policies.

The CJIS Audit Unit (CAU) will conduct triennial audits of each CSA in order to verify compliance with applicable statutes, regulations and policies. This audit includes a sample of Criminal Justice Agency (CJA) and NCJAs, in coordination with the SIB.

Note 1: Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with applicable statutes, regulations and policies.

Note 2: The FBI CJIS Division has the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

CSP Section 5.11.2 describes the requirements for the CSA to triennially audit all CJAs and NCJAs with direct access to the state system, establish a process to periodically audit all NCJAs with access to CJI, establish the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

CSP Section 5.11.3 describes the requirement that all agencies with access to CJI must permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations. The inspection team, appointed by the APB, will include at least one

representative of the CJIS Division. All results of the inquiry and audit will be reported to the APB with appropriate recommendations.

k. 5.12 – Personnel Security

CSP Section 5.12 provides agencies the security terms and requirements as they apply to all personnel who have unescorted access to unencrypted CJI, including individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI.

CSP Section 5.12.1 details the minimum screening requirements for all individuals requiring unescorted access to unencrypted CJI.

CSP Section 5.12.2 describes the requirement for an agency to immediately terminate CJI access for an individual upon termination of employment.

CSP Section 5.12.3 describes the requirement for an agency to review CJI access authorizations and initiate appropriate actions (such as closing and establishing accounts and changing system access authorizations) whenever personnel are reassigned or transferred to other positions within the agency.

CSP Section 5.12.4 describes the requirement for an agency to employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.

l. 5.13 – Mobile Devices

When access to CJI using mobile devices such as laptops, smartphones, and tablets is authorized, CSP Section 5.13 explains the controls required to manage those devices to ensure the information remains protected.

The following scenarios are intended to help the reader identify areas within the CSP that CJAs may often come across. Each scenario should be reviewed for applicability in conjunction with the above “General CJI Guidance” section. The specific requirements found with the CSP are not shown; however specific sections are referenced along with a requirements summary.

Hard Copy CJI Storage and Accessibility

When CJI is received in hard copy and the agency stores the paper within a locked file cabinet, the CJA should, in addition to the “General CJI Guidance”, focus on compliance with policy section:

a. 4.2.4 – Storage

When storing CJI, appropriate administrative, technical, and physical safeguards must be implemented to ensure the security and confidentiality of the information.

Electronic CJI Storage and Accessibility – Controlled Area

When an agency creates an electronic copy of CJI (e.g. scanning a document or creation of a spreadsheet) and subsequently stores this static CJI on either a local hard drive or shared network drive in a controlled area for indirect access by Authorized Recipients, the agency should, in addition to the “General CJI Guidance”, focus on compliance with policy section:

a. 5.5.2.4 (3) – Access Control Mechanisms – Encryption

CSP Section 5.5.2.4 item 3, Encryption – This describes the requirement for utilizing encryption as the primary access control mechanism which is necessary in this

situation. Encrypted information can only be read by personnel possessing the appropriate cryptographic key (e.g., passphrase) to decrypt. Refer to Section 5.10.1.2 for specific encryption requirements.

Electronic CJI Storage and Accessibility – Physically Secure Location

When an agency receives or creates an electronic copy of CJI and subsequently stores this CJI within a Records Management System (RMS), located within a physically secure location that may be queried by Authorized Recipients, the agency should, in addition to the “General CJI Guidance”, focus on compliance with policy sections:

a. **5.5 – Access Control**

CSP Section 5.5 describes the requirements and parameters for utilizing access control mechanisms for restricting CJI access (such as the reading, writing, processing and transmission of CJIS information) and the modification of information systems, applications, services and communication configurations allowing access to CJI to only authorized personnel.

b. **5.6 – Identification and Authentication**

CSP Section 5.6 describes the requirements and parameters agencies must implement to validate and authenticate the identity of information system users and processes acting on behalf of users the identities prior to granting access to CJI or agency information systems/services that process CJI.

c. **5.7 – Configuration Management**

CSP Section 5.7 describes the requirements for implementing access restrictions that will only permit authorized and qualified individuals access to information system components for purposes of initiating changes, including upgrades, and modifications.

CSP Section 5.7.1 describes the requirements for implementing the concept of least privilege (5.7.1.1) and for developing and maintaining network diagrams (5.7.1.2) that detail how the RMS is interconnected and protected within the network. See Appendix C for sample network diagrams.

CSP Section 5.7.2 details the requirement for agencies to protect the system documentation from unauthorized access consistent with the provisions described in Section 5.5 Access Control.

d. **5.10 – System and Communications Protection and Information Integrity**

CSP Section 5.10 details the requirements for network infrastructures within physically secure locations through establishment of system and communication boundary and transmission protection safeguards that assist in securing an agency’s environment, even when virtualized. In addition, this section describes the requirements for providing the capability to ensure system integrity through the detection and protection against unauthorized changes to software and information for applications, services, and information systems.

Use Case Scenarios

1. Indirect Access to Criminal Justice Information (CJI) Stored on a Network Server

A county court scans hard copy case documents containing CJI into an electronic format. The documents are placed on a network server which is located in a secure data center within the court offices. The data center meets all the requirements to be labeled a physically secure location as defined in Section 5.9.1 of the CSP.

Keeping in mind the scenario as described, an authorized user needs access to case documents. This user is not located in the secure data center and will have to use remote access to access the file. The user is therefore required to provide identification and authentication credentials to prove they are an authorized user. To access the documents, the user is prompted to enter their unique username and password. Because the documents reside on a system with indirect access to CJI (does not allow the user to query a state or national criminal record repository), AA is not required for access to the documents.

NOTE: If the Authorized User has direct access to CJI (the ability to query a state or national criminal record repository) in the above scenario, AA would be required.

2. Encryption for Data at Rest (Exemption for FIPS 140-2 Certified Encryption)

A county court scans hard copy case documents containing CJI in an electronic format. The documents are placed on a network server which is not located in a secure data center. Because the data center does not meet the requirements of a physically secure location, as defined in Section 5.9.1 of the CSP, the files, at rest (in storage) on the server, are required to be encrypted.

To prevent unauthorized access, the IT staff has decided to encrypt the entire folder that contains the files. They will use a product that provides an advanced encryption standard (AES) algorithm at 256 bit strength to comply with the CSP and employ a CSP compliant passphrase to lock the folder's encryption. When an authorized user needs to access to the case documents, they access the folder on the server and are prompted to enter the designated passphrase to decrypt (unlock) the folder. The user can then access all files within the folder. Additionally, because the documents reside on a system with indirect access to CJI (does not allow the user to query a state or national criminal record repository), AA is not required for access to the documents.

NOTE: Whenever authorized personnel no longer require access to the encrypted folder, the passphrase must be changed to prevent future access by that user.