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: _____