#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
5.10	**System and Communications Protection and Information Integrity**					
1.	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. Refer to CSP 5.13.4 for additional system integrity requirements related to mobile devices used to access CJI/CHRI. Based on inquiry and record examination, does the Tribe or TGRA's network infrastructure control the flow of information between interconnected systems?[1]	____	____	____	CSP 5.10.1	
	Based on inquiry and record examination, does the Tribe or TGRA utilize boundary protection?[2]	____	____	____	CSP 5.10.1	
2.	Does the Tribe or TGRA:					
	1. Control access to networks processing CJI/CHRI?	____	____	____	CSP5.10.1.1(1)	
	2. Monitor and control communications at the external boundary of the information system and at key internal boundaries within the system?	____	____	____	CSP5.10.1.1(2)	
	3. Ensure any connections to the Internet, other external networks, or information systems occur through controlled interfaces?[3]	____	____	____	CSP5.10.1.1(3)	
	4. Employ tools and techniques to monitor network events, detect attacks, and provide identification of unauthorized use?	____	____	____	CSP 5.10.1.1(4)	

[1] 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 CSP 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.

[2] 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.

[3] For example: proxies, gateways, routers, firewalls, encrypted tunnels. *See* CSP Section 5.13.4.3 for guidance on personal firewalls.

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
	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”)?	____	____	____	CSP 5.10.1.1(5)	
	6. Allocate publicly accessible information system[4] components (e.g. public Web servers) to separate sub networks with separate, network interfaces?	____	____	____	CSP 5.10.1.1(6)	
3.	Based on inquiry and record examination, when CJI/CHRI is transmitted outside the boundary of the physically secure location[5], does the Tribe or TGRA immediately protect the data via encryption[6]?	____	____	____	CSP 5.10.1.2.1	

[4] Publicly accessible information systems residing on a virtual host shall follow the guidance in CSP 5.10.3.2 to achieve separation.

[5] 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/CHRI and associated information systems.

[6] 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:
1. 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.
2. 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.
3. 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.

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
4.	Based on inquiry and record examination, when CJI/CHRI is at rest (i.e. stored digitally) outside the boundary of the physically secure location, does the Tribe or TGRA encrypt CJI/CHRI in accordance with CSP Section 5.10.1.2.1 (see above), or use a symmetric cipher that is FIPS 197 certified (AES) and at least 256 bit strength?	____	____	____	CSP 5.10.1.2.2	
	1. When the Tribe or TGRA implements encryption on CJI/CHRI at rest, does the passphrase used to unlock the cipher meet the following requirements:					
	a. Be at least 10 characters?	____	____	____	CSP 5.10.1.2.2(1)(a)	
	b. Not be a dictionary word?	____	____	____	CSP 5.10.1.2.2(1)(b)	
	c. Include at least one (1) upper case letter, one (1) lower case letter, one (1) number, and one (1) special character?	____	____	____	CSP 5.10.1.2.2(1)(c)	
	d. Be changed when previously authorized personnel no longer require access?	____	____	____	CSP 5.10.1.2.2(1)(d)	
	2. Do multiple files maintained in the same unencrypted folder have separate and distinct passphrases?[7] A single passphrase may be used to encrypt an entire folder or disk containing multiple files.	____	____	____	CSP5.10.1.2.2(2)	
5.	Based on inquiry and record examination, does the Tribe or TGRA use public key infrastructure (PKI) technology?	____	____	____	CSP5.10.1.2.3	
	If yes, does the Tribe or TGRA implement a certificate policy and certification practice statement for the issuance of public key certificates used in the information system?	____	____	____	CSP 5.10.1.2.3	
	If yes, does the registration to receive a public key certificate:					
	1. Include authorization by a supervisor or a responsible official?	____	____	____	CSP 5.10.1.2.3(1)	

[7] All audit requirements found in CSP 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.

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
	2. Be accomplished by a secure process that verifies the identity of the certificate holder?	____	____	____	CSP 5.10.1.2.3(2)	
	3. Ensure the certificate is issued to the intended party?	____	____	____	CSP 5.10.1.2.3(3)	
6.	Based on inquiry and record examination, does the Tribe or TGRA:					
	1. Implement network-based and/or host-based intrusion detection[8] or prevention[9] tools?	____	____	____	CSP 5.10.1.3(1)	
	2. Maintain current intrusion detection or prevention signatures?	____	____	____	CSP 5.10.1.3(2)	
	3. Monitor inbound and outbound communications for unusual or unauthorized activities?	____	____	____	CSP 5.10.1.3(3)	
	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?	____	____	____	CSP 5.10.1.3(4)	
	5. Review intrusion detection or prevention logs weekly or implement automated event notification?	____	____	____	CSP 5.10.1.3(5)	
	6. Employ automated tools to support near-real-time analysis of events in support of detecting system-level attacks?	____	____	____	CSP 5.10.1.3(6)	

[8] 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 to notify 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).

[9] 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.

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
7.	Based on inquiry and record examination, does the Tribe or TGRA deploy VoIP[10] within a network that contains unencrypted CJI/CHRI?	____	____	____	CSP 5.10.1.4	
	If yes, in addition to the security controls described in the CSP, are the following additional controls implemented:					
	1. Establish usage restrictions and implementation guidance[11] for VoIP technologies?	____	____	____	CSP 5.10.1.4(1)	
	2. Change the default administrative password on the IP phones and VoIP switches?	____	____	____	CSP 5.10.1.4(2)	
	3. Utilize Virtual Local Area Network (VLAN) technology to segment VoIP traffic from data traffic?	____	____	____	CSP 5.10.1.4(3)	
8.	Based on inquiry and record examination, does the Tribe or TGRA utilize cloud computing?[12]	____	____	____	CSP 5.10.1.5	
	If yes, does the Tribe or TGRA only permit the storage of CJI/CHRI, regardless of encryption status, 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))[13]?	____	____	____	CSP 5.10.1.5	

[10] 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. CSP Appendix G.2 outlines threats, vulnerabilities, mitigations, and NIST best practices for VoIP.

[11] CSP Appendix G.2 outlines threats, vulnerabilities, mitigations, and NIST best practices for VoIP.

[12] 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 CSP.

[13] This restriction does not apply to exchanges of CJI/CHRI 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).

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
	If yes, is Metadata derived from unencrypted CJI/CHRI protected in the same manner as CJI/CHRI and not used for any advertising or other commercial purposes by any cloud service provider or other associated entity?	____	____	____	CSP 5.10.1.5	
	If yes and applicable, does the Tribe or TGRA permit limited use of metadata derived from unencrypted CJI/CHRI when specifically approved by the Tribe/TGRA and its "intended use" is detailed within the service agreement?[14]	____	____	____	CSP 5.10.1.5	
9.	Based on inquiry and record examination, does the Tribe or TGRA transmit CJI/CHRI via a single or multi-function device over a standard telephone line?	____	____	____	CSP 5.10.2	
	If yes, CJI/CHRI transmitted via a single or multi-function device over a standard telephone line is exempt from encryption requirements.					
	Based on inquiry and record examination, does the Tribe or TGRA transmit CJI/CHRI externally to a physically secure location using a facsimile server, application or service which implements email-like technology?	____	____	____	CSP 5.10.2	
	If yes, CJI/CHRI transmitted externally 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 CSP 5.10.					
10.	Based on inquiry and record examination, does the Tribe or TGRA use advanced software to create virtual machines or partition applications, services, and system administration to reduce the amount of hardware needed for information systems?	____	____	____	CSP 5.10.3.1	

[14] 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.

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
	If yes, does the Tribe or TGRA separate the application, service or information systems user functionality (including user interface services) from information system management functionality?	____	____	____	CSP 5.10.3.1	
	Does the Tribe or TGRA separate, physically or logically, the application, service, or information system user interface services (e.g. public web pages) from information storage and management services (e.g. database management)?	____	____	____	CSP 5.10.3.1	
	Separation may be accomplished through the use of one or more of the following:					
	1. Different computers?	____	____	____	CSP 5.10.3.1(1)	
	2. Different central processing units?	____	____	____	CSP 5.10.3.1(2)	
	3. Different instances of the operating system?	____	____	____	CSP 5.10.3.1(3)	
	4. Different network addresses?	____	____	____	CSP 5.10.3.1(4)	
	5. Other methods approved by the FBI CJIS ISO?	____	____	____	CSP 5.10.3.1(5)	
11.	Based on inquiry and record examination, does the Tribe or TGRA use virtualization[15] to divide the resources of a computer (hardware and software) into multiple execution environments?	____	____	____	CSP 5.10.3.2	
	If yes, in addition to the security controls described in the CSP, are the following additional controls implemented by the Tribe or TGRA in a virtual environment?					
	1. Isolate the host from the virtual machine. In other words, virtual machine users cannot access host files, firmware, etc.?	____	____	____	CSP 5.10.3.2(1)	
	2. Maintain audit logs for all virtual machines and hosts and store the logs outside the hosts' virtual environment?	____	____	____	CSP 5.10.3.2(2)	
	3. Virtual Machines that are Internet facing (web servers, portal servers, etc.) physically separate from Virtual Machines (VMs) that process CJI/CHRI internally or separated by a virtual firewall?	____	____	____	CSP 5.10.3.2(3)	

[15] 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.

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
	4. Drivers that serve critical functions stored within the specific VM they service?[16]	____	____	____	CSP 5.10.3.2(4)	
	Additionally, are the following technical security controls applied in virtual environments where CJI/CHRI is comingled with non-CJI/CHRI:					
	1. Encrypt CJI/CHRI when stored in a virtualized environment where CJI/CHRI is comingled with non-CJI/CHRI or segregate and store unencrypted CJI/CHRI within its own secure VM?	____	____	____	CSP 5.10.3.2(1)	
	2. Encrypt network traffic within the virtual environment?	____	____	____	CSP 5.10.3.2(2)	
	Lastly, are the following technical security controls and best practices implemented wherever feasible:					
	1. Implement IDS and/or IPS monitoring within the virtual environment?	____	____	____	CSP 5.10.3.2(1)	
	2. Virtually or physically firewall each VM within the virtual environment to ensure that only allowed protocols will transact?	____	____	____	CSP 5.10.3.2(2)	
	3. Segregate the administrative duties for the host?	____	____	____	CSP 5.10.3.2(3)	
12.	Based on inquiry and record examination, does the Tribe or TGRA identify applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws?	____	____	____	CSP 5.10.4.1	
	Based on inquiry and record examination, does the Tribe or TGRA (or the software developer/contractor in the case of software developed and maintained by a contractor) develop and implement a local policy that ensures prompt installation of newly released security relevant patches[17], service packs and hot fixes?	____	____	____	CSP 5.10.4.1	

[16] 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.

[17] Patch requirements discovered during security assessments, continuous monitoring or incident response activities shall also be addressed expeditiously.

Sample Audit Checklist for CJIS Security Policy Area 10

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
	The local policies of the Tribe or TGRA(or the software developer/contractor), should include such items as:					
	1. Testing of appropriate patches before installation?	____	____	____	CSP 5.10.4.1(1)	
	2. Rollback capabilities when installing patches, updates, etc?	____	____	____	CSP 5.10.4.1(2)	
	3. Automatic updates without individual user intervention?	____	____	____	CSP 5.10.4.1(3)	
	4. Centralized patch management?	____	____	____	CSP 5.10.4.1(4)	
13.	Based on inquiry and record examination, does the Tribe or TGRA implement malicious code protection that includes automatic updates for all systems with Internet access?	____	____	____	CSP 5.10.4.2	
	Based on inquiry and record examination, for systems not connected to the Internet, does the Tribe or TGRA implement local procedures to ensure malicious code protection is kept current (i.e. most recent update available)?	____	____	____	CSP 5.10.4.2	
	Based on inquiry and record examination, does the Tribe or TGRA 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?	____	____	____	CSP 5.10.4.2	
	Based on inquiry and record examination, does the Tribe or TGRA ensure malicious code protection is enabled on all of the aforementioned critical points and information systems and resident scanning employed?	____	____	____	CSP 5.10.4.2	
14.	Based on inquiry and record examination, does the Tribe or TGRA implement spam and spyware protection?	____	____	____	CSP 5.10.4.3	
	Based on inquiry and record examination, does the Tribe or TGRA:					
	1. Employ spam protection mechanisms at critical information system entry points (e.g. firewalls, electronic mail servers, remote-access servers)?	____	____	____	CSP 5.10.4.3(1)	
	2. Employ spyware protection at workstations, servers and mobile computing devices on the network?	____	____	____	CSP 5.10.4.3(2)	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
	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 the CSP?	____	____	____	CSP 5.10.4.3(3)	
15.	Based on inquiry and record examination, does the Tribe or TGRA:					
	1. Receive information system security alerts/advisories on a regular basis?	____	____	____	CSP 5.10.4.4(1)	
	2. Issue alerts/advisories to appropriate personnel?	____	____	____	CSP 5.10.4.4(2)	
	3. Document the types of actions to be taken in response to security alerts/advisories?	____	____	____	CSP 5.10.4.4(3)	
	4. Take appropriate actions in response?	____	____	____	CSP 5.10.4.4(4)	
	5. Employ automated mechanisms to make security alert and advisory information available throughout the agency as appropriate?	____	____	____	CSP 5.10.4.4(5)	
16.	Based on inquiry and record examination, does the Tribe or TGRA restrict the information input to any connection to FBI CJIS services to authorized personnel only?[18]	____	____	____	CSP 5.10.4.5	

[18] 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.