NCJITS Pre-Audit

Preview

Report created: Wed Jul 10 2024 06:59:45 GMT-0700 (Pacific Daylight Time)

Section - Section 1: Supporting documentation to be included as part of the audit

1. Outsourcing Certifications (if applicable) - signed confirmation from each contractor with unescorted access to unencrypted CHRI confirming receipt/understanding of the CJIS Security Policy and Outsourcing Standard.

□ Yes
□ No
□ N/A

2. Outsourcing Audits (if applicable) - audit documentation of the 90-day audit of contractors storing and/or processing CHRI unescorted.

□ Yes
□ No
□ N/A

3. Personnel Sanctions Policy - rules of acceptable use of CHRI and/or disciplinary actions for misuse.

○ Yes
○ No

4. Awareness Training List - (include: first and last name, date of hire, date of last training, user role[Individual with unescorted access to a physically secure locations, General User, Privileged User, Organizational Personnel with Security Responsibilities administrator, query-only, etc.], agency, and department).

○ Yes
○ No

5. Awareness Training Materials - (if applicable) provide if the Tribe or TGRA creates curriculum.

□ Yes
□ No
□ N/A

6. Physical Protection Policies and Procedures - a written policy that describes the agency's physical protections for CHRI (i.e., visitors are escorted, no unauthorized access in secure areas, etc.).

○ Yes
○ No

7. Physical ("paper") and Digital Media Protection Policies and Procedures- to include handling, storage, transport, sanitization, and disposal/destruction (Where is media stored? How is it moved from one secure location to another? How is it destroyed? Who destroys?).

○ Yes
○ No

8. Network Diagram - high-level diagram that shows all forms of FBI CJIS systems access [including wireless, dial-up, etc.] by system users and/or IT personnel. (Do not include specific IP addresses).

○ Yes
○ No

9. Event Logs - (if applicable) screen shot or word document containing a sample of the event logs for each information system managed by the Tribe/TGRA accessing CHRI (successful and unsuccessful log on attempts, password changes, transactions, etc.).

□ Yes
□ No
□ N/A

10. Procedures/Forms for requesting and/or removing access to Information Systems – include account management policies and procedures (how does a user get an account, what happens when a user is transferred or terminated, account validation procedures, how a user is approved for remote access with privileged functions, etc.).

○ Yes
○ No

11. Procedures for Security Incident Reporting/Handling - written procedures for reporting a breach of CHRI; include any documentation for security incidents reported within the last three years.

○ Yes
○ No

Section - Section 2: Administration of Noncriminal Justice Functions

1. Does the Tribe or TGRA have access to CHRI by means other than the 2021 CHRI MOU?

○ Yes
○ No

Primary question answered Yes

1. If yes, how?

2. Does the Tribe or TGRA retain or store the results (hard copies or electronic) of the CHRI and/or documents containing criminal history record results?

○ Yes
○ No

Primary question answered Yes

1. If yes, how?

□ Hard copy (licensing files, filing cabinet)
□ Email (kept on email server/archive)
□ Scanned (shared network access)
□ Saved to desktop (not on network file share)
□ Other

3. Does the Tribe or TGRA disseminate the results to the individual of record? (i.e., Do you give the results to the person you requested the record on?).

○ Yes
○ No

Primary question answered Yes

1. If yes, how?

□ Mail (hard copy)
□ Courier service
□ Hand carried by authorized personnel
□ Email
□ Verbal (face to face / over the phone)

4. Does the Tribe or TGRA disseminate the results to any other entity/individual? (e.g., another similar agency, accreditation, private contractors, etc.).

○ Yes
○ No

Primary question answered Yes

1. a. If yes, who?
1. Contractor
2. Another agency
3. Legal counsel
4. TGRA meeting / public license hearing
5.Other:___________________________

b. If yes, how?
1. Mail / Courier Service
2. Hand carried by authorized personnel
3. Email
4. Verbal (face to face / over the phone)
5. Other:__________________________

c. If yes, why are the results provided to the entity/individual and for what purpose?

5. Does the Tribe or TGRA outsource for any noncriminal justice administrative functions?

○ Yes
○ No

Primary question answered Yes

1. If yes, what functions are outsourced?

□ Data destruction (paper shredding, hard drives)
□ IT services (network/system administration, desktop support, Live Scan etc.)
□ Off-site media storage (data centers, backup, cloud storage, paper storage archives, etc.)
□ Eligibility determinations
□ Other

6. Does the Tribe or TGRA have a contract/agreement with the contractor(s), which incorporates or references the CJIS Security Policy and Outsourcing Standard?

○ Yes
○ No

7. Has the Tribe or TGRA ensured each contractor has confirmed, in writing, he/she understands the Outsourcing Standard requirements?

○ Yes
○ No

8. Has the Tribe or TGRA ensured the contractor keeps/maintains the signed certification for the Outsourcing Standard requirements for each employee in a file?

○ Yes
○ No

9. Does the Tribe or TGRA ensure that the contractor maintains an updated list of personnel who have access to CHRI?

○ Yes
○ No

10. Does the Tribe or TGRA ensure the contractor notifies the Tribe or TGRA within 24 hours when additions and/or deletions occur?

○ Yes
○ No

Section - Section 3: Responsibilities if a contractor has access to CHRI

1. Does the Tribe or TGRA monitor the contractor's compliance with the terms and conditions of the Outsourcing Standard?

○ Yes
○ No

2. Does the Tribe or TGRA conduct an audit of the contractor within 90 days of the date the contractor first receives CHRI under the outsourcing agreement?

○ Yes
○ No

3. Has the Tribe or TGRA had to terminate a contract?

○ Yes
○ No

Primary question answered Yes

1. If yes, did the Tribe or TGRA, within four hours, notify the FBI Compact Officer of any security violation or termination of the contract?

○ Yes
○ No

2. If yes, did the Tribe or TGRA provided written notice to the FBI Compact Officer?

○ Yes
○ No

4. Has the Tribe or TGRA's contractor experienced a PII breach?

○ Yes
○ No

Primary question answered Yes

1. If yes, did the Tribe or TGRA notify the FBI CJIS ISO within an hour of the breach?

○ Yes
○ No

2. If yes, did the Tribe or TGRA provide a report to the FBI CJIS ISO within five calendar days of the breach?

○ Yes
○ No

5. Does the Tribe or TGRA ensure the contractor makes its facilities available for announced and unannounced audits by the Tribe or TGRA and/or the FBI on behalf of the Compact Council?

○ Yes
○ No

6. Does the contractor maintain CHRI?

○ Yes
○ No

Primary question answered Yes

1. If yes, does the contractor maintain CHRI only for the period of time necessary to fulfill its contractual obligations?

○ Yes
○ No

7. Does the Contractor disseminate CHRI?

○ Yes
○ No

Primary question answered Yes

1. If yes, does the Contractor have consent from the Tribe or TGRA to disseminate CHRI?

○ Yes
○ No

2. If yes, does the Contractor maintain a log of the disseminated CHRI for a minimum one-year retention period?

○ Yes
○ No

3. If yes, does the log concerning the dissemination of CHRI clearly identify the following?

□ Tribe or TGRA with unique identifiers to include the NIGC Originating Agency Identifier (ORI) or Originating Agency Case (OCA) of the Tribe or TGRA?
□ Date of dissemination
□ Means of dissemination

Section - Section 4: Information Protection – Personnel Security, Awareness Training, Security Incidents and Violations, Media Protection and Disposal, Physical Security

1. Does the Tribe or TGRA have a written policy for the discipline of personnel failing to comply with established information security policies and procedures (i.e., misuse of the system)?

○ Yes
○ No

2. Does the Tribe or TGRA provide security and privacy literacy training to system users (including managers, senior executives, and contractors) as part of initial training for new users prior to the users accessing CJI and annually thereafter?

○ Yes
○ No

Primary question answered Yes

1. If yes, is documentation of individual awareness training maintained, to include contractors, if applicable?

○ Yes
○ No

3. What are the procedures when a security violation or incident is detected?

4. Does the Tribe or TGRA report the security violation or incident to anyone?

○ Yes
○ No

Primary question answered Yes

1. If yes, who?

5. Does the Tribe or TGRA ensure general incident response roles and responsibilities are included in as part of required security awareness training for all authorized personnel and contractors, if applicable?

○ Yes
○ No

6. Does the Tribe or TGRA have written incident response procedures?

○ Yes
○ No

7. Has the Tribe or TGRA reported/had any security violations or incidents in the last three years? (Incidents in which security of CHRI was compromised or put at risk).

○ Yes
○ No

Primary question answered Yes

1. If yes, please provide the details of the violation(s) and or incident(s):

8. Describe the location(s) where CHRI is retained and how it is retained. (e.g., locked file cabinet, locked office, off-site storage facility, records archive, etc.).

Is each location physically secure to prevent unauthorized access?

9. Does the Tribe or TGRA store files that contain CHRI in an off-site record storage facility?

○ Yes
○ No

Primary question answered Yes

1. If yes, who owns/manages the facility? (i.e., who controls access).

2. If yes, how are the records stored at the off-site facility?

10. Does the Tribe or TGRA 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

11. Does the Tribe or TGRA ensure authorized personnel escort visitors in physically secure locations at all times (in all access and storage areas to include off-site facilities if designated physically secure)?

○ Yes
○ No

12. How does the Tribe or TGRA dispose of non-digital (hard copy/paper) media containing CHRI?

13. Does the Tribe or TGRA have written procedures for physical media destruction?

○ Yes
○ No

14. If authorized personnel do not conduct the sanitization or destruction of the non-digital media, is the process witnessed by authorized personnel?

○ Yes
○ No

15. When digital media reaches end of life (no longer works) or is to be replaced/upgraded, how does the Tribe or TGRA destroy the media (e.g., hard drives, thumb drives, CDs, etc.)?

16. Does the Tribe or TGRA have written procedures for the sanitization and/or destruction of digital media?

○ Yes
○ No

17. If authorized personnel do not conduct the sanitization or destruction of the digital media, is the process witnessed by authorized personnel?

○ Yes
○ No

18. Describe the physical location(s) where computer(s) with access to CHRI are stored.(e.g., locked office, reception area, etc.)

Is each location physically secure to prevent unauthorized access?

19. Does the Tribe or TGRA ensure digital media with CHRI is encrypted in transit and at rest outside a physically secure location or controlled area?

○ Yes
○ No

Primary question answered Yes

1. If encryption is used, describe the method (bit level, hardware/software, etc.) of encryption. (e.g., Adobe Pro, WinZip, TrueCrypt, etc.).

2. If encryption is used, does the Tribe or TGRA protect the information using a passphrase (to unlock encryption)? Please describe.

20. Does the Tribe or TGRA 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

21. Does the Tribe or TGRA store or back up digital media with CHRI to an off-site storage or a disaster recovery location?

○ Yes
○ No

Primary question answered Yes

1. If yes, who owns/manages the facility? (i.e., who controls access).

2. If yes, describe how the digital media with CHRI is transported to the off-site storage or disaster recovery location. (i.e., disc to disc with encryption or physical tapes encrypted or in locked box, etc.).

3. If yes, describe how the digital media with CHRI is stored at the off-site storage or disaster recovery location?

Section - Section 5: Network Infrastructure

1. Does the Tribe or TGRA maintain and regularly update and protect a network diagram?

○ Yes
○ No

2. Does the Tribe or TGRA prohibit the use of personally owned digital media devices on all agency owned or controlled systems that store, process, or transmit CHRI?

○ Yes
○ No

3. Does the Tribe or TGRA allow publicly owned computers to access, process, store, or transmit CHRI? (Publicly accessible computers include but are not limited to hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.)?

○ Yes
○ No

4. Does the Tribe or TGRA ensure all information systems accessing CHRI display an approved system use notification message that includes the following?

1. The user is accessing 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.

Does the approved system use notification message remain on the screen until the user acknowledges the notification?

5. Does the Tribe or TGRA, for information systems managed by them, ensure each user enters a basic password that conforms to all of the following standards?

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 User id.
4. Expire within a maximum of 90 calendar days.
5. Not be identical to the previous ten (10) passwords.
6. Not be transmitted in clear text outside the secure location.
7. Not be displayed when entered.

Please identify the information systems managed by the Tribe or TGRA (e.g. network, record management systems, etc.).

6. For information systems managed by the Tribe or TGRA that access CHRI, has the Tribe or TGRA implemented “advanced password standards” in lieu of “basic password standards”?

○ Yes
○ No

Primary question answered Yes

1. If yes, do the advanced password standards meet all the CJISSECPOL 5.6.2.1.1.2 requirements?

○ Yes
○ No

7. Does the Tribe or TGRA allow users or IT administrators to share usernames or passwords or have generic group accounts?

○ Yes
○ No

8. Describe the Tribe or TGRA process for issuing user accounts, deleting/disabling user accounts, and periodic validation of user accounts.

9. Does the Tribe or TGRA have a written policy that describes their account management process?

○ Yes
○ No

10. Do the information systems managed by the Tribe or TGRA initiate a session lock (require the user to re-enter password) after a maximum of 30 minutes of inactivity?

○ Yes
○ No

Primary question answered No

1. When a user leaves a computer, does the user initiate a session lock or log out of the information system?

○ Yes
○ No

11. For information systems managed by the Tribe or TGRA, do they enforce a limit of no more than five consecutive invalid access attempts by a user (attempting to access CHRI or systems with access to CHRI)?

○ Yes
○ No

12. Does the Tribe or TGRA ensure that the application or information system automatically lock the account/node for a10-minute time period unless released by an administrator?

○ Yes
○ No

13. Do the information systems managed by the Tribe or TGRA accessing CHRI generate audit records for defined events?

In the event the Tribe or TGRA does not use an automated system, manual recording of activities must still take place.

○ Yes
○ No

14. Do the Tribe or TGRA managed information systems accessing CHRI log the following events?

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

Please identify the information systems managed by the Tribe or TGRA (e.g., network, record management systems, etc.).

15. Does the Tribe or TGRA ensure the content of every audited event includes the date, time, component (where it occurred), type of event, user and the outcome (success or failure) of the event?

If a misuse or unauthorized release of CHRI were to occur, could the Tribe or TGRA identify the individual responsible for the security incident?

16. Does the Tribe or TGRA conduct weekly audits of records on information systems managed by them that store or access CHRI?

○ Yes
○ No

17. Does the Tribe or TGRA retain the audit records for at least one year?

○ Yes
○ No

18. Does the Tribe or TGRA allow the transit of CHRI outside a physically secure location(s) or controlled area(s) on managed information systems?

If yes, how is the CHRI encrypted [1] (e.g. method of encryption, bit level, hardware/software)?

If yes, does the Tribe or TGRA use a FIPS 140-2 certified cryptographic module?

To retrieve the certificate for the FIPS 140-2 validated cryptographic module, complete the following steps:

1. Visit http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm
2. Locate your cryptographic module vendor and product.
3. Click on "Certificate Number" and print.

Please submit a copy of any applicable encryption certificates with this completed pre-audit questionnaire or have the certificates available at the time of the audit.

[1] The CJIS Security Policy requires that all CJIS data transmitted through any public network segment or over dial-up or Internet connections shall be immediately protected with a minimum 128-bit encryption. Systems that transmit data over radio frequencies to a network with access to CJIS data are also subject to this requirement. This 128-bit encryption must be certified by the National Institute of Standards and Technology (NIST) or Canada's Communications Security Establishment (CSE) to ensure that the cryptographic modules meet Federal Information Processing Standard (FIPS) 140-2 certification requirements.

19. Does the Tribe or TGRA use wireless network devices to access CHRI?

○ Yes
○ No

Primary question answered Yes

1. If yes, please identify the device types:

□ Laptops (large form factor) (used for remote access/maintenance)
□ Tablets/iPads (medium form factor)
□ Smartphones (small form factor)
□ Other:

20. Does the Tribe or TGRA ensure each laptop or large form factor mobile devices (i.e., devices with full-feature operating systems) employ a personal firewall and malicious code protection?

○ Yes
○ No

21. Does the Tribe or TGRA ensure medium or small form factor mobile devices (i.e., devices that do NOT have a full-feature operating system use a mobile device manager (MDM) for configuration control, application usage, device protection and recovery)?

○ Yes
○ No

Primary question answered Yes

1. If yes, does the MDM satisfy the listed requirements?

○ Yes
○ No

22. Does the Tribe or TGRA monitor mobile devices not capable of an always –on cellular connection to ensure their patch and update state is current?

○ Yes
○ No

23. Does the Tribe or TGRA authorize cellular devices that have access to CHRI for use outside of the U.S.?

○ Yes
○ No

Primary question answered Yes

1. If yes, does the Tribe or TGRA perform a documented inspection to ensure all controls are in place and functioning properly in accordance with the Tribe's or TGRA's policies prior to and after deployment outside of the U.S?

○ Yes
○ No

24. Describe the Tribe's or TGRA's boundary protection used to protect the network (i.e., hardware/software firewalls, proxies, gateways, guards, routers, etc.).

25. Does the Tribe or TGRA ensure access to CHRI is separate from Non-CHRI related access (i.e., can unauthorized users access CHRI information systems on a Virtual Local Area Network (VLAN) or from other interconnected systems?

○ Yes
○ No

Primary question answered Yes

1. If yes, how?

26. Has the Tribe or TGRA implemented network-based and/or host-based intrusion detections tools?

○ Yes
○ No

Primary question answered Yes

1. If yes, does Tribe or TGRA ensure the following tools:

1. Maintain current signatures.
2. Monitor inbound and outbound communications for unusual or unauthorized activities.
3. Send individual intrusion detection logs to a central logging facility where correlation and analysis will be accomplished as a system wide intrusion detection effort.
4. Review intrusion detection or prevention logs weekly or implement automated event notification.
5. Employ automated tools to support near-real-time analysis of events in support of detecting system level attacks.

○ Yes
○ No

27. Does the Tribe or TGRA implement malicious code protection that includes automatic updates for all CHRI information systems with Internet access?

If N/A, CHRI information systems not connected to the Internet must implement local procedures to ensure malicious code protection is kept current (i.e., most recent update available).

□ Yes
□ No
□ N/A

28. Does the Tribe or TGRA implement spam and spyware protection?

○ Yes
○ No

29. Does the Tribe or TGRA stay up to date with relevant security alerts and advisories?

○ Yes
○ No

30. Does the Tribe or TGRA apply routine patches and updates to all software and components? (i.e., Windows updates, firewall patches, etc.).

○ Yes
○ No

31. Does the Tribe or TGRA host any CHRI in a virtualized [1] environment?

[1] 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.

○ Yes
○ No

Primary question answered Yes

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

32. Does the Tribe or TGRA utilize a cloud provider to host or store CHRI related information systems, applications, or data?

○ Yes
○ No

Primary question answered Yes

1. If yes, what service do they provide?

1. Software as a Service (SaaS).
2. Platform as a Service (PaaS).
3. Infrastructure as a Service (IaaS).
4. Other:

Please provide details including services provided (in relation to CHRI) as well as details of how the Tribe or TGRA protects the cloud environment.