State of Texas – CJIS Security Office - SaaS Assessment Process

This process is to be used by law enforcement agencies for all "Agency" proposed cloud-based solutions used to process, store, or transmit Criminal Justice Information (CJI).
The Agency must receive a formal Notice of Compliance issued by the DPS CJIS Technical Compliance Analysts before the proposed cloud-based solution is used to process, store, or transmit CJI.

THE TIMELINE FOR THE COMPLETION OF THE SaaS ASSESSMENT IS PRIMARILY CONTINGENT UPON THE QUALITY OF AGENCY RESPONSES TO THE ONLINE SaaS ASSESSMENT QUESTIONNAIRE.
TO EXPEDITE THE PROCESS: PLEASE ASK FOR VENDOR ASSISTANCE IN THE COMPLETION OF THE QUESTIONNAIRE AND DOCUMENT FINDINGS IN THE AGENCY SECURITY PLAN FOR THE SaaS SOLUTION.

SaaS ASSESSMENT STARTED

Once the agency decides upon a Vendor SaaS solution used to process, store, or transmit CJI, the Agency should review this process, the relevant security controls outlined in the CJIS Security Policy Requirements Companion Document, and contact DPS if you have additional questions.
Once the Agency signs a Vendor contract for the SaaS solution, the Vendor should sign the Texas version of the CJIS Security Addendum with the Agency which legally binds the Vendor and Vendor personnel working on the contract, to the requirements of the CJIS Security Policy, the State of Texas CJIS Security Policy Supplement, and any enhanced Agency security requirements.

The Vendor should provide the Agency a Security Plan for the proposed SaaS solution that details how the proposed solution is configured to meet the current CJIS Security Policy requirements and enhanced Agency security requirements.

THE SECURITY PLAN SHOULD BE REVIEWED BY THE AGENCY PRIOR TO SIGNING THE CONTRACT TO ENSURE THE PROPOSED SOLUTION CAN MEET CJIS SECURITY POLICY REQUIREMENTS WHICH IS ALWAYS THE AGENCY RESPONSIBILITY

We Trust, But Verify!

Required Documentation

Documents should be sent to cjis.assessments@dps.texas.gov

- Cloud-Service Provider (CSP) Enrollment Agreement or any contractual paperwork between Vendor and CSP validating SaaS solution is hosted in a government cloud.
- Agency Network Diagram including Proposed SaaS Solution, with an updated equipment list: *(Make, Model. OS/firmware version, Date Last Updated, End of Support Date)*
- A copy of the fully executed CJIS Security Addendum.
- CJIS Online – Certification Status Report showing all Vendor personnel are current with required Awareness Training
- Documented step-by-step Remote Access procedures for all methods and all Vendor personnel granted Remote Access.
- Vendor personnel list including least-privilege permissions granted.
- A copy of all CJI data sharing agreements, currently in use, and via proposed solution.
- A copy of the agency Remote Access, BYOD, MDM, Account Management, Incident Response Plan, and Sanctions policy and any other documentation needed by DPS to complete the assessment.
- Request for a TEST connection

Effective 01/01/2024
CJIS Security Office (512) 424-5686
Http://dps.texas.gov/securityreview

DPS will not formally start an SaaS Assessment unless the Agency has provided DPS a fully executed CJIS Security Addendum with the Vendor

The Agency submits request for SaaS Assessment to CJIS Technical Compliance Analysts with a copy of the fully executed CJIS Security Addendum between the Agency and the Vendor, and all Required Documentation

If you are unsure who signs the CJIS Security Addendum, follow the money; who pays the bills?

DPS will confirm the Texas version of the CJIS Security Addendum is Fully Executed

Yes

No

Agency needs to submit a fully executed Security Addendum:

Page 1 - Contact Information
Page 2-6 - Legal Jargon
Page 7 – FBI Certification Pages
Page 8 – Texas Signatory Page

The Agency confirms Vendor personnel successfully completed the appropriate level of Awareness Training and sent CJIS Online Certification Status Report to DPS for review

Yes

DPS will confirm Awareness Training of Vendor personnel has been successfully completed

No

Agency needs to validate Vendor personnel completed the appropriate level of Awareness Training and sent CJIS Online Certification Status Report to DPS for review

CSP personnel do not have access to CJI and do not require Agency Personnel Screening

The Agency must meet the minimum CJIS Security Policy requirements, or risk potential CSA sanctions.

The Agency conducted Vendor Personnel Screening identified by the FBI Certification Pages of the Security Addendum

Yes

DPS will confirm Personnel Screening of Vendor personnel is complete and all are eligible for least -privileged access

No

Agency needs to validate all vendor staff working on the contract with access to unencrypted CJI and/or systems used to process CJI have completed Personnel Screening and manage personnel changes

Need More Information or Non Compliant

The DPS CJIS Technical Compliance Analyst will assign the Agency an online SaaS Assessment Questionnaire for the proposed solution in the CJIS Technical Audit Portal.
The agency will receive an email with a link to the Assessment.
Credentials will be established by DPS and provided only to the Agency designee.

The Agency will need to work with Vendor to complete the online SaaS Assessment ensuring all responses provide sufficient details as to how the assessed security control requirement has been met by the Agency.
Once complete, submit Assessment Questionnaire responses in the online CJIS Technical Audit Portal to DPS for review.
Update the Security Plan as changes are being made. You will need this for your next audit.

NO LIMIT

CJIS Compliance Analysts confirm all assessed security controls meet CJIS/DPS security requirements.

Approved

Agency proposed solution is approved to connect to TLETS systems to process, store, and/or transmit CJI.

The DPS CJIS Technical Compliance Analyst will notify the Agency and TLETS letting them know they have approved the specific interface(s) as outlined in the assessment of the Agency proposed solution.

SaaS ASSESSMENT COMPLETED

Agency will work with TLETS to complete any interface connections issues for Test and/or Production use.

DPS WILL AUDIT AND ASSESS ANY UPDATES TO THE SOLUTION DURING THE NEXT CJIS TECHNICAL AUDIT

THIS IS WHERE THE PROCESS MAY SLOW DOWN

The Agency must provide detailed responses to how the proposed solution is being configured to meet CJIS requirements for the assessed security control(s).

The Vendors like to respond by saying in their Security Plan that it is the Agency responsibility to meet many of the assessed security control(s), which is true, but it does not explain how the solution meets the assessed security control(s). Regardless, the Agency needs to provide detailed response that will explain how the proposed solution will be configured to meet the CJIS requirements of the assessed security control(s).

The Agency should request the Vendor provide detailed responses to all relevant security controls for the proposed solution which can be found in the current version of the CJIS Security Policy Requirements Companion document.
Or, the Vendor can wait until the assessment begins and work with the Agency to respond to the assessment questionnaire, which will likely take longer…

v5.9.3 SaaS Assessment

Preview

Report created: Tue Jan 23 2024 16:31:03 GMT-0600 (Central Standard Time)

Section - Agency Information

1. Please provide agency name, agency contact information and ORI

2. Please provide vendor name and contact information

3. Is this solution a new interface or is it a replacement for an existing product?

4. Please indicate if the agency proposed solution involves a direct interface to TLETS.

- ○ Yes
- ○ No

5. Please give a brief description of the proposed vendor solution

6. Please provide a list of vendor modules (i.e.: CAD/RMS/JMS/Data Sharing/etc. included in the assessment.

7. Please acknowledge, only those modules listed above are included in the assessment.

Additional modules must be assessed by DPS prior to the agency using the new module for processing CJI.

☐ I have read and agree to the above statement.

8. Please provide the name of the Cloud Service Provider (CSP) hosting the SaaS solution for the vendor.

NOTE: All cloud-based services used to process, store, and/or transmit CJI must be hosted in a DPS approved government cloud.

9. Please confirm, since the agency has the contract with the vendor, the agency is required to take the lead on all negotiations with the vendor(s) in order to proceed with this assessment.

NOTE: The CJIS Security Office will not discuss agency specific details of the agency proposed solution with the vendor unless an agency representative is included in the discussions.

☐ I have read and agree to the above statement.

10. Will you need a test interface?

○ Yes
○ No

Primary question answered Yes

1. If so, by what date?

11. What is your desired go-live date? Please be aware that this is subject to the approval process time, which varies.

Section - Policy Area 1 - Information Exchange Agreements

1. 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 of the CJIS Security Policy 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.

☐ I have read and understand the above statement.

2. 5.1.1.4 Interagency and Management Control Agreements

Does the agency share CJI with other agencies, or any other entities?

○ Yes
○ No

Primary question answered Yes

1. Please indicate what software solution(s) are used to share CJI.
Please provide your auditor copies of all Interagency Agreements between the agency and any other entities in which CJI is being shared.

5.1.3) If the agency is involved in secondary dissemination of CHRI to an agency that is not party to an existing agreement, please provide the auditor a snippet from the secondary dissemination log of the releasing agency.

3. 5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum

Does the agency have a Security Addendum for all vendor personnel with access to agency secure locations or systems used to process CJI?

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 of the CJISSECPOL. 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).

- ○ YES
- ○ NO
- ○ NA

Primary question answer 1 selected

1. Please indicate below who the Security Addendum is with and email a signed, fully executed copy of the entire document (along with vendor employee FBI certification pages) to your auditor.

Primary question answer 2 selected

1. A Security Addendum is required for agencies which are supported through third party vendors or contractors for services (non-law enforcement support for IT services, etc.) when unescorted access or remote access is made available for vendor personnel to any system on the agency secure network.

Please describe how support is provided for the agency. (example; escort only, etc.)

Primary question answer 3 selected

1. Please explain the reason you selected N/A

Section - Policy Area 2 - Awareness and Training (AT)

1. AT-3 AWARENESS AND TRAINING

Have all vendor personnel successfully completed appropriate role-based awareness training?

All individuals with unescorted access to a physically secure location;

General User: A user who is authorized to use an information system

Privileged User: A user that is authorized (and, therefore, trusted) to perform security-relevant functions that general users are not authorized to perform

Organizational Personnel with Security Responsibilities: Personnel with the responsibility to ensure the confidentiality, integrity, and availability of CJI and the implementation of technology in a manner compliant with the CJISSECPOL. (i.e., LASO)

○ Yes
○ No

Primary question answered Yes

1. Please describe below the methods used, (ie; CJIS Online, etc.)

2. Please provide the auditor a copy of the CJIS Online Certification Status Report for all vendor personnel working on this proposed solution

☐ I have read and will comply.

Section - Policy Area 3 - Incident Response

1. 5.3 Incident Response

Does the agency have a copy of the vendor's documented incident response plan detailing incident handling, collection of evidence, incident response training, and incident monitoring?

○ Yes
○ No

Primary question answered Yes

1. Please provide a copy of the documented Incident Response Plan to your auditor.

☐ I have read and will comply.

Section - Policy Area 4 - Auditing and Accountability

1. Please describe the process the agency follows to obtain audit records from the cloud service provider for defined events as described below?

5.4.1.1 Events

Are the following events logged and kept for a minimum of one year (365 days)?

Successful and unsuccessful system log-on attempts.
Successful and unsuccessful attempts to access,create, write, delete or change permission on a user account, file, directory or other system resource.
Successful and unsuccessful attempts to change account passwords.
Successful and unsuccessful actions by privileged accounts.
Successful and unsuccessful attempts for users to access, modify, or destroy the audit log file.

5.4.1.1.1 Content

Is the following content included with every audited event?

Date and time of the event.
The component of the information system (e.g.,software component, hardware component) where the event occurred.
Type of event.
User/subject identity.
Outcome (success or failure) of the event

2. Has the agency confirmed the vendor maintains audit logs meeting the following requirements?

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.

○ Yes
○ No

Section - Policy Area 5 - Access Control (AC)

1. AC-2 Account Management

Does the Agency:

a. Define and document the types of accounts allowed and specifically prohibited for use within the system;
b. Assign account managers;
c. Require conditions for group and role membership;
d. Specify:

1. Authorized users of the system;
2. Group and role membership; and
e. Require approvals by organizational personnel with account management responsibilities for requests to create accounts;
f. Create, enable, modify, disable, and remove accounts in accordance with agency policy;
g. Monitor the use of accounts;
i. Authorize access to the system based on:
1. A valid access authorization;
2. Intended system usage; and
j. Review accounts for compliance with account management requirements at least annually;
k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and
l. Align account management processes with personnel termination and transfer processes.

- ○ YES
- ○ NO
- ○ NA

2. AC-2 (4) Automated Audit Actions

Does the agency automatically audit account creation, modification, enabling, disabling, and removal actions?

- ○ Yes
- ○ No

3. AC-4 Information Flow Enforcement

Does the agency enforce approved authorizations for controlling the flow of information within the system and between connected systems by preventing CJI from being transmitted unencrypted across the public network, blocking outside traffic that claims to be from within the agency, and not passing any web requests to the public network that are not from the agency-controlled or internal boundary protection devices (e.g., proxies, gateways, firewalls, or routers)?

- ○ Yes
- ○ No

4. AC-5 Separation of Duties

Does the agency:

a. Identify and document separation of duties based on specific duties, operations, or information systems, as necessary, to mitigate risk to CJI; and
b. Define system access authorizations to support separation of duties?

- ○ Yes
- ○ No

5. AC-6 Least Privilege

Does the agency employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks?

- ○ Yes
- ○ No

6. AC-6 (1) Authorize Access to Security Functions

Does the agency authorize access for personnel including security administrators, system and network administrators, and other privileged users with access to system control, monitoring, or administration functions (e.g., system administrators, information security personnel, maintainers, system programmers, etc.) to:
(a) Established system accounts, configured access authorizations (i.e., permissions, privileges), set events to be audited, set intrusion detection parameters, and other security functions; and
(b) Security-relevant information in hardware, software, and firmware.

○ Yes
○ No

7. AC-6 (2) Non-privileged Access For Nonsecurity Functions

Does the agency require that users of system accounts (or roles) with access to privileged security functions or security-relevant information (e.g., audit logs), use non-privileged accounts or roles, when accessing non-security functions?

○ Yes
○ No

Primary question answered Yes

1. Please provide your auditor a list of non-privileged accounts assigned to personnel that also have privileged access.

8. AC-6 (5) Privileged Accounts

Does the agency restrict privileged accounts on the system to privileged users?

○ Yes
○ No

9. AC-6 (9) Log Use of Privileged Functions

Does the agency log the execution of privileged functions?

○ Yes
○ No

10. AC-6 (10) Prohibit Non-Privileged Users From Executing Privileged Functions

Does the agency prevent non-privileged users from executing privileged functions?

○ Yes
○ No

11. AC-7 Unsuccessful Logon Attempts

Does the agency:
a. Enforce a limit of five (5) consecutive invalid logon attempts by a user during a 15-minute time period; and
b. Automatically lock the account or node until released by an administrator when the maximum number of unsuccessful attempts is exceeded?

○ Yes
○ No

12. AC-8 System Use Notification

Does the system display a system use notification message to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that:
1. Users are 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 subject to criminal and civil penalties; and
4. Use of the system indicates consent to monitoring and recording;
b. Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system; and
c. For publicly accessible systems:
1. Display system use information consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines, before granting further access to the publicly accessible system;
2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
3. Include a description of the authorized uses of the system.

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

NOTE: This includes any connected device(s) including MBIS, Live Scan, and ULW.

○ YES
○ NO
○ NA

Primary question answer 1 selected

1. Please email your auditor a copy of the System Use Notification message as it is displayed on the screen.

☐ I have read and will comply.

13. AC-11 Device Lock

Does the information system accessing CJI:

a. Prevent further access to the system by initiating a device lock after a maximum of 30 minutes of inactivity and requiring the user to initiate a device lock before leaving the system unattended?

NOTE: 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.

b. Retain the device lock until the user reestablishes access using established identification and authentication procedures?

NOTE: This includes any connected device(s) including MBIS, Live Scan, and ULW.

Note Exemptions; MDTs (PatrolVehicles), Dispatch, and Receive Only Terminals (ROT).

○ YES
○ NO
○ NA

14. AC-11 (1) Pattern-Hiding Displays

Does the information system conceal, via the device lock, information previously visible on the display with a publicly viewable image?

○ Yes
○ No
○ N/A

15. AC-17 Remote Access

Has the agency:

a. Established and documented usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and
b. Authorized each type of remote access to the system prior to allowing such connections?

NOTE: This includes any connected device(s) including MBIS, Live Scan, and ULW.

○ YES
○ NO
○ NA

Primary question answer 1 selected

1. Please provide your auditor a copy of the agency remote access policy and documented technical and administrative (step-by-step) process for enabling remote access. Please include the applicable FIPS Certificate numbers for CJI In Transit in relation to the remote solution and method of AA/MFA being used.

☐ I have read and will comply.

16. AC-18 Wireless Access

Does the agency:

a. Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; and
b. Authorize each type of wireless access to the system prior to allowing such connections?

○ Yes
○ No

17. AC-18 (1) Authentication and Encryption

Does the agency protect wireless access to the system using authentication of authorized users and agency-controlled devices, and encryption?

○ Yes
○ No

Section - Policy Area 6 - Identification and Authentication (IA)

1. IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

Does the agency uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of users in order to ensure detailed accountability of individual activity?

- ○ Yes
- ○ No

2. IA-2 DEVICE IDENTIFICATION AND AUTHENTICATION

Does the agency uniquely identify agency-managed devices before establishing network connections?

- ○ Yes
- ○ No

3. IA-2(1) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | MULTIFACTOR AUTHENTICATION TO PRIVILEGED ACCOUNTS

Please provide a brief description of the agency plans to implement multi-factor authentication for access to privileged accounts. If the agency has established a timeline to meet the pending requirement, please include the anticipated "go-live" date.

Multi-Factor Authentication requires the use of two or more different factors to achieve authentication:
1) Something you know (e.g.,PIN)
2) Something you have (e.g., physical authenticator such as a cryptographic key)
3) Something you are (e.g., biometric)

4. IA-2(2) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | MULTIFACTOR AUTHENTICATION TO NON-PRIVILEGED ACCOUNTS

Please provide a brief description of the agency plans to implement multi-factor authentication for access to non-privileged accounts. If the agency has established a timeline to meet the pending requirement, please include the anticipated "go-live" date.

Multi-Factor Authentication requires the use of two or more different factors to achieve authentication:
1) Something you know (e.g.,PIN)
2) Something you have (e.g., physical authenticator such as a cryptographic key)
3) Something you are (e.g., biometric)

5. IA-4 IDENTIFIER MANAGEMENT

Does the agency manage system identifiers (individual, group, role, service, device) and prevent reuse of identifiers for one (1) year?

○ Yes
○ No

6. IA-5 AUTHENTICATOR MANAGEMENT

Does the agency manage system authenticators by:
a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator;
b. Establishing initial authenticator content for any authenticators issued by the organization;
c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;
e. Changing default authenticators prior to first use;
f. Changing or refreshing authenticators annually or when there is evidence of authenticator compromise;
g. Protecting authenticator content from unauthorized disclosure and modification;
h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and
i. Changing authenticators for group or role accounts when membership to those accounts changes.

○ Yes
○ No

7. IA-5(1) AUTHENTICATOR MANAGEMENT | AUTHENTICATOR TYPES

Please select all of the Authenticator Types currently in use by the agency:

Below is a list of the current CJISSECPOL security controls:

(a) Memorized Secret Authenticators and Verifiers:
(1) Maintain a list of commonly-used, expected, or compromised passwords and update the list quarterly and when organizational passwords are suspected to have been compromised directly or indirectly;
(5) Enforce the following composition and complexity rules: when agencies elect to follow basic password standards.
(a) Not be a proper name.
(b) Not be the same as the Userid.
(c) Expire within a maximum of 90 calendar days.
(d) Not be identical to the previous ten (10) passwords.
(e) Not be displayed when entered.
6. If chosen by the subscriber, memorized secrets SHALL be at least 8 characters in length.
7. If chosen by the CSP or verifier using an approved random number generator, memorized secrets SHALL be at least 6 characters in length.
8. Truncation of the secret SHALL NOT be performed.
9. Memorized secret verifiers SHALL NOT permit the subscriber to store a “hint” that is accessible to an unauthenticated claimant.
10. Verifiers SHALL NOT prompt subscribers to use specific types of information (e.g., “What was the name of your first pet?”) when choosing memorized secrets.
11. When processing requests to establish and change memorized secrets, verifiers SHALL compare the prospective secrets against a list that contains values known to be commonly used, expected, or compromised.
12. If a chosen secret is found in the list, the CSP or verifier SHALL advise the subscriber that

they need to select a different secret.
13. If a chosen secret is found in the list, the CSP or verifier SHALL provide the reason for rejection.
14. If a chosen secret is found in the list, the CSP or verifier SHALL require the subscriber to choose a different value.
15. Verifiers SHALL implement a rate-limiting mechanism that effectively limits failed authentication attempts that can be made on the subscriber's account to no more than five.
16. Verifiers SHALL force a change of memorized secret if there is evidence of compromise of the authenticator.
17. The verifier SHALL use approved encryption when requesting memorized secrets in order to provide resistance to eavesdropping and MitM attacks.
18. The verifier SHALL use an authenticated protected channel when requesting memorized secrets in order to provide resistance to eavesdropping and MitM attacks.
19. Verifiers SHALL store memorized secrets in a form that is resistant to offline attacks.
20. Memorized secrets SHALL be salted and hashed using a suitable one-way key derivation function.
21. The salt SHALL be at least 32 bits in length and be chosen arbitrarily to minimize salt value collisions among stored hashes.
22. Both the salt value and the resulting hash SHALL be stored for each subscriber using a memorized secret authenticator

(b) Look-up Secrets Authenticators and Verifiers
{Not auditable/santionable until 10/01/2024}

(c) Out-of-Band Authenticators and Verifiers
{Not auditable/santionable until 10/01/2024}

(d) OTP Authenticators and Verifiers
d(4) The authenticator output SHALL have at least 6 decimal digits (approximately 20 bits) of entropy.
d(6) The OTP value associated with a given nonce SHALL be accepted only once.

(e) Cryptographic Authenticators and Verifiers (including single- and multi-factor cryptographic authenticators, both hardware- and software-based)
{Not auditable/santionable until 10/01/2024}

☐ (a) Memorized Secret Authenticators and Verifiers
☐ (b) Look-up Secrets Authenticators and Verifiers
☐ (c) Out-of-Band Authenticators and Verifiers
☐ (d) OTP Authenticators and Verifiers
☐ (e) Cryptographic Authenticators and Verifiers (including single- and multi-factor cryptographic authenticators, both hardware- and software-based)

8. IA-5(2) AUTHENTICATOR MANAGEMENT | PUBLIC KEY-BASED AUTHENTICATION

Does the agency utilize public key-based authentication or public key infrastructure (PKI)?

○ Yes
○ No
○ N/A

Primary question answer 1 selected

1. Does the agency:
(a) For public key-based authentication:
1. Enforce authorized access to the corresponding private key; and
2. Map the authenticated identity to the account of the individual or group; and
(b) When public key infrastructure (PKI) is used:
1. Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; and
2. Implement a local cache of revocation data to support path discovery and validation.

○ Yes
○ No

9. IA-6 AUTHENTICATION FEEDBACK

Does the agency obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals (e.g. masking - displaying asterisks when the user types the password)?

○ Yes
○ No

10. IA-8 IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)

Does the agency uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users?

○ Yes
○ No

11. Please acknowledge the agency has reviewed the CJIS Security Policy (CJISSECPOL) version 5.9.3 and is fully aware of the security controls within the IA-IDENTIFICATION AND AUTHENTICATION section that are not yet auditable/sanctionable.

☐ I have read and understand the above statement.

Section - Policy Area 7 - Configuration Management

1. 5.7.1.2 Network Diagram

Does the agency have a proposed Network Diagram to include the SaaS solution,which also includes 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.

Please describe any physical equipment or logical segmentation (VLANs, ACLs, etc.) providing segmentation and list the FIPS 140-2 certificate numbers on the network diagram where encryption of CJI In Transit is in use.

○ YES
○ NO
○ NA

Primary question answer 1 selected

1. Please send the auditor a current (updated) agency network diagram for review. Please also include an equipment list of all agency equipment on the network diagram, detailing the equipment Make, Model, OS/Firmware Version, Date Last Updated, End of Support Date.

☐ I have read and will comply.

Section - Policy Area 8 - Media Protection (MP)

1. MP-1 POLICY AND PROCEDURES

Does the agency have documented media protection policy that addresses purpose, scope, roles, responsibilities, management commitment,coordination among agency entities, and compliance; and is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
does the agency have documented procedures to facilitate the implementation of the media protection policy and the associated media protection controls; and
has the agency designated an individual with security responsibilities to manage the development, documentation, and dissemination of the media protection policy and procedures?

Please send a copy of the Media Protection Policy to the auditor.

○ Yes
○ No

2. MP-2 MEDIA ACCESS

Does the agency restrict access to digital and non-digital media to authorized individuals?

○ Yes
○ No

3. MP-4 MEDIA STORAGE

Does the agency physically control and securely store digital and non-digital media within physically secure locations or controlled areas and encrypt CJI on digital media when physical and personnel restrictions are not feasible; and
protect system digital and non-digital media until the media are destroyed or sanitized using approved equipment, techniques, and procedures?

○ Yes
○ No

4. MP-5 MEDIA TRANSPORT

Does the agency protect and control digital (flash drives, external hard drives) and non-digital media (micro-film, paper) to help prevent compromise of the data during transport outside of the physically secure locations or controlled areas using encryption; and restrict the activities associated with transport of system, electronic, and physical media to authorized personnel maintaining accountability for system media during transport outside of the physically secure location or controlled areas; and documents the activities associated with the transport of system media?

○ Yes
○ No

5. Please acknowledge the agency has reviewed the CJIS Security Policy (CJISSECPOL) version 5.9.3 and is fully aware of the security controls within the MP-MEDIA PROTECTION section that are not yet auditable/sanctionable. Specifically MP-3 MEDIA MARKINGS.

☐ I have read and understand the above statement.

Section - Policy Area 9 - Physical Protection

Section - Policy Area 10: System and Communications Protection and Information Integrity

1. 5.10.1.1 Boundary Protection

Does the agency have a boundary protection device (firewall) implemented to protect computers and access devices from non-CJI networks that meets at a minimum:

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 subnetworks with separate, network interfaces. Publicly accessible information systems residing on a virtual host shall follow the guidance in Section5.10.3.2 to achieve separation.

- ○ YES
- ○ NO
- ○ NA

Primary question answer 1 selected

1. Briefly describe equipment or software in use by the agency to meet boundary requirements. Information should include Make, Model and firmware of any device(s) in use or software brand and version.

2. 5.10.1.2 Encryption

Does the agency encrypt all CJI data before it leaves the secure location?

- ○ YES
- ○ NO
- ○ NA

3. 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 128bit strength to protect CJI.

Does the agency encrypt all CJI data to meet FIPS 140-2 standards before transmission outside of the secure network?

○ YES
○ NO
○ NA

Primary question answer 1 selected

1. Provide relevant FIPS 140-2 details and Certificate numbers below:

4. 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, the agency 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.

Does the agency encrypt all CJI data at Rest?

○ YES
○ NO
○ NA

Primary question answer 1 selected

1. Provide relevant details or Certificate numbers below

5. 5.10.1.3 Intrusion Detection Tools and Techniques

Does the agency implement intrusion prevention systems at the perimeter of the secure network which meets at a minimum:

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.

○ Yes
○ No

6. 5.10.3.1 Partitioning

Are applications, services, or information services physically or logically separate?

Separation may be accomplished through the use of one or more of the following:

Different Computers

Different Central Processing Units

Different instances of the operating system

Different network addresses

Other methods approved by the FBI CJIS ISO

○ YES
○ NO
○ NA

Section - Policy Area 11 - Formal Audits

Section - Policy Area 12 - Personnel Security

1. 5.12 Personnel Security

Have all vendor personnel who access CJIS Data either physically, logically, or remotely been fingerprint based background checked by the agency prior to being granted access?

○ Yes
○ No

Section - Policy Area 13 - Mobile Devices

1. 5.13 Mobile Devices*

Has the agency established written usage restrictions and implementation guidelines for wireless technologies? (ex: BYOD policy or local SOP, MDM Policy).

○ YES
○ NO
○ NA

Primary question answer 1 selected

1. Please ensure a copy of the local policy or SOP is provided to your auditor for review.

☐ I have read and will comply.

2. 5.13.1.1 All 802.XX Wireless Protocols

If applicable, has the agency implemented 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 AreaNetwork (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 non essential 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.

○ YES
○ NO
○ NA

3. 5.13.1.4 Mobile Hotspots

If applicable, does the agency allow mobile devices that are approved to access or store CJI to function as a Wi-Fi hotspot connecting to the Internet, meet at a minimum configuration:

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.

○ YES
○ NO
○ NA

4. 5.13.2 Mobile Device Management (MDM)

If Mobile Device Management (MDM) is in use, does it meet at a minimum the following compensating controls:

Remote locking of device

Remote wiping of device

Setting and locking device configuration

Detection of "rooted" or "jailbroken" devices

Enforce folder and/or disk level encryption

Application of mandatory policy settings on the device

Detection of unauthorized configurations

Detection of unauthorized software or applications

Ability to determine the location of agency controlled devices

Prevention of unpatched devices from accessing CJI or CJI systems

Automatic device wiping after a specified number of failed attempts

○ YES
○ NO
○ NA

Primary question answer 1 selected

1. Provide details below regarding type and software solution in use for MDM.

5. 5.13.3 Wireless Device Risk Mitigations

If applicable, utilizing wireless devices - Has the agency established at a minimum the following risk controls:

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.

- ○ Yes
- ○ No
- ○ N/A

6. 5.13.4.3 Personal Firewall

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).

Does the firewall, at a minimum, 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.

- ○ YES
- ○ NO
- ○ NA

Primary question answer 1 selected

1. Please provide brief description of Firewall solution in place.

(IE; Built-in Windows firewall, software name, etc.)

7. 5.13.5 Incident Response (Mobile Devices)

In addition to the requirements in Section 5.3 Incident Response, agencies are responsible to meet additional reporting and handling procedures.

Has the agency developed a written plan which includes Special reporting procedures for mobile devices 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 compromiseoutside the United States

○ YES
○ NO
○ NA

Primary question answer 1 selected

1. Please provide (if not already submitted) a copy of the agency's Incident Response Plan which covers mobile devices (Handhelds / Tablets) to your auditor.

☐ I have read and will comply.

8. 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.

Is Advanced Authentication (AA) in use?

○ YES
○ NO
○ NA

Primary question answer 1 selected

1. Provide software solution and details of what AA solution is in place at the agency below.

9. 5.13.7.2.1 Compensating Controls

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.

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.

Within the State of Texas, CSO approved compensating controls to meet the AA requirement on agency-issued smartphones and tablets with limited feature operating systems are permitted. This request must be submitted via email to the resource: security.committee@dps.texas.gov and must include within the body of the email what measures (see below) are in place as well as the product name and version.

If applicable, does the agency's MDM solution meet the following minimum 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

○ YES
○ NO
○ NA

Section - Policy Area 14 - System and Service Acquisition (SA)

1. SA-22 UNSUPPORTED SYSTEM COMPONENTS

Does the agency replace system components when support for the components is no longer available from the developer, vendor, or manufacturer?

○ Yes
○ No
○ N/A

Primary question answer 2 selected

1. Please explain how the agency provides support for unsupported components.

Primary question answer 3 selected

1. Please explain the reason for selecting "N/A"?

Section - Policy Area 15 - System and Information Integrity (SI)

1. SI-2 FLAW REMEDIATION

Does the agency:
a. Identify, report, and correct system flaws;
b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
c. Install security-relevant software and firmware updates within the number of days listed after the release of the updates;
• Critical – 15 days
• High – 30 days
• Medium – 60 days
• Low – 90 days; and
d. Incorporate flaw remediation into the organizational configuration management process.

○ Yes
○ No

2. SA-22 UNSUPPORTED SYSTEM COMPONENTS
(2) FLAW REMEDIATION | AUTOMATED FLAW REMEDIATION STATUS

Does the agency:
Determine if system components have applicable security-relevant software and firmware updates installed using vulnerability scanning tools as least quarterly or following any security incidents involving CJI or systems used to process, store, or transmit CJI?

○ Yes
○ No

3. SI-10 INFORMATION INPUT VALIDATION

Does the agency:
Check the validity of the following information inputs: all inputs to web/application servers, database servers, and any system or application input that might receive or process CJI.

○ Yes
○ No

4. SI-11 ERROR HANDLING

Does the agency:
a. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited; and
b. Reveal error messages only to organizational personnel with information security responsibilities.

○ Yes
○ No