Show without Compliance Responses

Technical Security Audit Cycle 21

Section: 1. Agency LEADS Access

1). How does your agency access LEADS? Check all that apply 1-3 or 4.

* This question is not assessed for compliance. It's for information only.

» (Choose All That Apply)

- We have LEADS 2000 terminals
- We have MDTs/Laptops
- We have Tablets/smartphones
- None of the above - we use another agency for LEADS access

Compliance Response
No Compliance Response Found

Section: 2. Roles and Responsibilities

1). As the designated Local Agency Security Officer (LASO), are you aware of your responsibilities as outlined in the CJIS Security Policy v. 5.8?

- Yes
- No

Compliance Response
Attention, this is an informational only question and you will not be marked out-of-compliance for this response. There is no further action you can take other than to educate the LASO on their duties.

It is important that the Local Agency Security Officer (LASO) understands his/her roles within each Terminal Agency. The CJIS Security Policy identifies the roles and responsibilities of the LASO; however, this is the minimum set of responsibilities and agencies may assign a greater number of roles to the LASO as it sees fit. The minimum set of roles and responsibilities of the LASO as identified in ***CJIS Security Policy v. 5.8 Section 3.2.9*** are as follows:

Each LASO shall:

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

2). Do you have the most current version of the CJIS Security Policy (CSP v. 5.8)?

Note: This is an informational question only and your answer will not be checked for compliance. You may download the most current version of the CJIS Security Policy at https://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view

- Yes
- No

Compliance Response
No Compliance Response Found

Section: 3. Required Policies

1). Does your Agency have a written Computer Incident Response policy and process in place including procedures to report incidents to appropriate agency officials and/or authorities?

- Yes
- No

Compliance Response
Please refer to CJIS Security Policy v. 5.8 Section 5.3.

2). Does your agency have a written policy for the procedures to dispose of digital media that may contain criminal justice information?

- Yes
- No

Compliance Response
Please refer to CJIS Security Policy v. 5.8 Section 5.8.3.

3). Does your agency have a written policy for the disposal of physical media that contains criminal justice information such as rap sheets, case reports and incident reports?

- Yes
- No

Compliance Response
Please refer to CJIS Security Policy v. 5.8 Section 5.8.4.

4). Does your agency have a written policy for physical access control to non-public areas, and that verifies the authorization of the person prior to granting him/her access?

- Yes
- No

Compliance Response
Please refer to CJIS Security Policy v. 5.8 Section 5.9.

5). Does your agency have written policies, based on state and local privacy rules, that ensures appropriate controls are applied when handling PII extracted from Criminal Justice Information (CJI)?

"Personally Identifiable Information (PII) is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name." (*CJIS Security Policy v. 5.8 Section 4.3*)

- Yes
- No

Compliance Response
Please refer to CJIS Security Policy v. 5.8 section 4.3.

Section: 4. Information Technology Services

1). Has your Agency designated a Non-Criminal Justice Agency (NCJA government) to perform information technology functions on your behalf, such as a city or county IT Department?

- Yes
- No

Compliance Response
No Compliance Response Found

» Primary question answered Yes

1). Have the appropriate staff at the NCJA undergone a criminal justice applicant fingerprint-based State and Federal background checks within 30 days of assignment?

- Yes
- No

Compliance Response

Please refer to CJIS Security Policy v5.7 Section 5.12.

2). Are all NCJA staff who are under the management control of the criminal justice agency current with their appropriate level of security awareness training?

- Yes
- No

Compliance Response
Please refer to CJIS Security Policy v5.7 Section 5.2.

The Illinois State Police provides online security awareness training for all levels. To access security awareness training please visit www.cjisonline.com

3). Does your agency have an inter-agency agreement with the non-criminal justice agency which contains language placing the non-criminal justice employees under the management control of your agency?

Management Control means a criminal justice agency shall have the authority to set, maintain, and enforce:

1. Priorities
2. Standards for the selection, supervision, and termination of personnel access to criminal justice information.
3. Policy governing operation of justice systems, computers, access devices, circuits, hubs, routers, firewalls, and any other components, including encryption, that comprise and support a telecommunications network and related criminal justice systems to include but not limited to criminal history record/criminal justice information, insofar as the equipment is used to process or transmit criminal justice systems information guaranteeing the priority, integrity, and availability of service needed by the criminal justice community.
4. Restriction of unauthorized personnel from access or use of equipment accessing the State network.
5. Compliance with all rules and regulations of the criminal justice agency's policies and CJIS Security Policy in the operation of all information received.

- Yes
- No

Compliance Response
Please refer to CJIS Security Policy v5.7 Section 5.1.1.4.

2). Has your Agency designated a Private Contractor to perform information technology functions on your behalf?

- Yes
- No

Compliance Response

No Compliance Response Found

» Primary question answered Yes

1). Has the appropriate staff from the private vendor undergone a criminal justice applicant fingerprint-based State (of agency and of residence) and Federal background checks within 30 days of assignment?

The Illinois State Police will also accept background checks if conducted by another Illinois criminal justice agency.

- Yes
- No

Compliance Response

Please refer to CJIS Security Policy v5.8 Section 5.12.

2). Has each employee from the private vendor who performs work for your agency signed the FBI Security Addendum which you maintain for your records?

- Yes
- No

Compliance Response

Please refer to CJIS Security Policy v5.8 Section 5.1.1.5.

3). Are all employees of the private contractor who do work on your behalf current with their appropriate level of security awareness training?

- Yes
- No

Compliance Response

Please refer to CJIS Security Policy v5.8 Section 5.2.

The Illinois State Police provides online security awareness training for all levels. To access security awareness training please visit www.cjisonline.com

Section: 5. Personnel Security and Training

1). Have you conducted fingerprint-based State and Federal background check for all agency personnel who have unescorted access to CJ data?

- Yes
- No

Compliance Response

Please refer to CJIS Security Policy v5.7 Section 5.12.

2). Do you provide and maintain current records for all employees who are subject to Basic Security Awareness (Level 1) training?

These employees include maintenance, custodial staff, and any other person who has unescorted access to Physically Secure Locations.

» (Choose One Answer Only)

- Yes
- No
- We do not have any emloyees/contractors who have unescorted access around CJI.

Compliance Response

Please refer to CJIS Security Policy v5.7 Section 5.2.

The Illinois State Police provides online security awareness training for all levels. To access security awareness training please visit www.cjisonline.com

3). Do you provide and maintain current records for all employees who are subject to Level 4 Security Awareness training?

These employees include IT Staff who support and/or have ability to access criminal justice information or Physically Secure Locations.

If an agency doesn't have IT staff and doesn't use outside IT services (private or government) and has a staff member who occasionally performs support, troubleshooting, maintenance, etc., that person is subject to Level 4 Security Awareness requirement.

» (Choose One Answer Only)

- Yes
- No
- We do not have staff who support our systems with CJI.

Compliance Response

Please refer to CJIS Security Policy v5.7 Section 5.2.

The Illinois State Police provides online security awareness training for all levels. To access security awareness training please visit www.cjisonline.com

Section: 6. Auditing and Accountability

1). Each agency is responsible for identifying the systems which contain Criminal Justice Information (CJI), and once identified, ensure that certain events within those systems are maintained in an audit log. This can be done at the application level and/or the operating system level. Once the systems to be logged are identified the following events shall be logged:

1. Successful and unsuccessful system log-on attempts.
2. Successful and unsuccessful attempts to use:
a) access permission on a user account, file directory or other system resource;
b) create permission on a user account, file directory or other system resource;
c) write permission on a user account, file directory or other system resource;
d) delete permission on a user account, file directory or other system resource;
e) change permission on a user account, file directory or other system resource.
3. Successful and unsuccessful attempts to change account passwords.
4. Successful and unsuccessful actions by privileged accounts.
5. Successful and unsuccessful attempts for users to:
a) access the audit log file;
b) modify the audit log file;
c) destroy the audit log file.

Does your agency, or another agency on your behalf, or your IT vendor review the above information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions?

» (Choose One Answer Only)

- Yes
- No
- N/A

Compliance Response

The responsible management official shall designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions. Audit review/analysis shall be conducted at a minimum once a week. The frequency of review/analysis should be increased when the volume of an agency's processing indicates an elevated need for audit review. The agency shall increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to agency operation, agency assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information. (*CJIS Security Policy v. 5.8 Section 5.4.3*)

» Primary question answer 3 selected

1). Please explain why this question does not apply to your agency.

-

Compliance Response

The responsible management official shall designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions. Audit review/analysis shall be conducted at a minimum once a week. The frequency of review/analysis should be increased when the volume of an agency's processing indicates an elevated need for audit review. The agency shall increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to agency operation, agency assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information. (*CJIS Security Policy v. 5.8 Section 5.4.3*)

Section: 7. Access Control

1). Do you allow more than five (5) consecutive invalid login attempts for your systems that access Criminal Justice Data?

- Yes
- No

Compliance Response

Please refer to CJIS Security Policy v. 5.8 Section 5.5.3

2). Does your agency prevent further access to the system by initiating a session lock (for example a screen saver with password) after a maximum of 30 minutes of inactivity?

- Yes
- No

Compliance Response

Please refer to CJIS Security Policy v5.8 Section 5.5.5.

3). An Appropriate System Usage Notification is a banner, typically on login screens, which informs the user - prior to logging on - what is expected of them when using the system. Usually, the user must agree, either by checking a box or simply by logging in to the system, that he/she understands the appropriate

usage of the system and the data contained therein.

Do all your systems that access Criminal Justice Information display an Appropriate System Use Notification prior to the user signing on to the system?

- Yes
- No

Compliance Response

The information system shall display an approved system use notification message, before granting access, informing potential users of various usages and monitoring rules. The system use notification message shall, at a minimum, provide the following information:

1. The user is accessing a restricted information system.
2. System usage may be monitored, recorded, and subject to audit.
3. Unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties.
4. Use of the system indicates consent to monitoring and recording.

The system use notification message shall provide appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remain on the screen until the user acknowledges the notification and takes explicit actions to log on to the information system.

Privacy and security policies shall be consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidance. System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. For publicly accessible systems;

(i) the system use information is available and when appropriate, is displayed before granting access;
(ii) any references to monitoring, recording, or auditing are in keeping with privacy accommodations for such systems that generally prohibit those activities; and
(iii) the notice given to public users of the information system includes a description of the authorized uses of the system. (*CJIS Security Policy v. 5.8 Section 5.5.4*)

4). Do you allow remote access (for example VPN) into your systems? Remote access is any temporary access to an agency's information system by a user (or an information system) communicated temporarily through an external, non-agency-controlled network (e.g., the Internet).

- Yes
- No

Compliance Response

No Compliance Response Found

» Primary question answered Yes

1). Does your agency employ automated mechanisms to facilitate the monitoring and control of remote access methods?

- Yes
- No

Compliance Response

Please refer to CJIS Security Policy v5.8 Section 5.5.6.

The agency shall authorize, monitor and control all methods of remote access to the information system. Remote access is any temporary access to an agency's information system by a user (or an information system) communicating temporarily through an external, non-agency-controlled network (e.g., the Internet).

The agency shall employ automated mechanisms to facilitate the monitoring and control of remote access methods. The agency shall control all remote accesses through managed access control points. The agency may permit remote access for privileged functions only for compelling operational needs but shall document the technical and administrative process for

enabling remote access for privileged functions in the security plan for the information system.

Virtual escorting of privileged functions is permitted only when all the following conditions are met:

1. The session shall be monitored at all times by an authorized escort.
2. The escort shall be familiar with the system/area in which the work is being performed.
3. The escort shall have the ability to end the session at any time.
4. The remote administrative personnel connection shall be via an encrypted (FIPS 140-2 certified) path.
5. The remote administrative personnel shall be identified prior to access and authenticated prior to or during the session. This authentication may be accomplished prior to the session via an Advanced Authentication (AA) solution or during the session via active teleconference with the escort throughout the session*.*

2). Please describe circumstances and encryption strength used for remote access.

To find about the FIPS 140-2 encryption certification please begin at this website: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

-

Compliance Response
Is FIPS 140-2 encryption certificate available?

Section: 8. System Accounts and Passwords

1). Passwords used for systems accessing Criminal Justice Information must include security attributes. Do the passwords at your agency follow these guidelines: (*CJIS Security Policy v. 5.8 Section 5.6.2.1.1*)

1. Be a minimum 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 the clear outside the secure location.
7. Not be displayed when entered.

- Yes
- No

Compliance Response
Please refer to CJIS Security Policy v5.8 section 5.6.2.1.1.

2). Does your agency validate at least annually and document the validation process for information system accounts, making sure the users are active and their credentials are appropriate?

- Yes
- No

Compliance Response
Please refer to CJIS Security Policy v5.8 section 5.5.1.

3). Does the account management include identification of type (i.e., individual, group, system) and criteria for group membership?

- Yes
- No

Compliance Response

Please refer to CJIS Security Policy v5.8 section 5.5.1.

Section: 9. Configuration Management

1). Does your agency maintain a current network diagram that includes:

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 the 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?

- Yes
- No

Compliance Response
Please refer to CJIS Security Policy v. 5.8 Section 5.7.1.2.

2). Does your agency utilize an 802.11 wireless protocol within your facility?

- Yes
- No

Compliance Response
No Compliance Response Found

» Primary question answered Yes
1). Do you maintain a complete inventory of all Access Points and 802.11 wireless devices?

- Yes
- No

Compliance Response
Please refer to CJIS Security Policy v5.8 Section 5.13.1.1.

2). Does your agency change all the default passwords for your access points with a strong administrative password?

- Yes
- No

Compliance Response
Please refer to CJIS Security Policy v5.8 Section 5.13.1.1.

Section: 10. Physical Protection

1). Does your agency have any devices that can display criminal justice information and are accessible to the public, or placed where the public has the ability to view the criminal justice information?

- Yes

- No

Compliance Response

The agency shall control physical access to information system devices that display CJI and shall position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing CJI. (*CJIS Security Policy v. 5.8 Section 5.9.1.5*)

Section: 11. System and Communications Protection and Information Integrity

1). Does your agency allow users to email case/incident reports, rap sheets or any other document or file containing criminal justice information?

- Yes
- No

Compliance Response

No Compliance Response Found

» Primary question answered Yes

1). When emailing criminal justice information are the contents of the email encrypted utilizing FIPS 140-2 standards prior to sending the email?

- Yes
- No

Compliance Response

Please refer to CJIS Security Policy v. 5.8 Section 5.10.1.2

2). Does your agency utilize cloud computing for either storing or transmitting criminal justice information?

- Yes
- No

Compliance Response

No Compliance Response Found

» Primary question answered Yes

1). Does the cloud provider you're using meet all the requirements set forth in the CJIS Security Policy, including the requirements of a private contractor providing IT services to a Criminal Justice Agency?

- Yes
- No

Compliance Response

Please refer to CJIS Security Policy v. 5.8 Section 5.10.1.5.

3). Does your agency ensure that every device accessing your network employ some sort of Malicious Code Protection (anti-virus software) and ensure that the protection software is kept up-to-date?

- Yes
- No

Compliance Response

Please refer to CJIS Security Policy v. 5.8 Section 5.10.4.2.

4). Does your agency ensure that computers which access CJ data are being updated with all necessary software patches?

- Yes
- No

Compliance Response

Please refer to CJIS Security Policy v5.8 Section 5.10.4.1.

Section: 12. Mobile Devices

1). Do you have MDTs or laptops which are capable of running LEADS queries and are not permanently stored in secure locations?

* Note that a police vehicle is considered as a secure location.

- Yes
- No

Compliance Response

No Compliance Response Found

» Primary question answered Yes

1). Is Advanced Authentication implemented on the device?

Notes:

You should answer "NO" if you only have a user ID and password.

Advanced Authentication (or 2-Factor Authentication) requires additional information, for example a temporary PIN, bio-metric data, or a security certificate to name a few.
For bio-metric data such as fingerprint to be compliant it needs to be maintained by the agency.

Having a user ID/password for the device, and another user ID/password to access CJ data is not sufficient.

- Yes
- No

Compliance Response

Please refer to CJIS Security Policy v5.8 Section 5.6.2.2.

2). Do you use mobile devices such as tablets or smartphones to access or process CJ data?

- Yes
- No

Compliance Response

No Compliance Response Found

» Primary question answered Yes

1). Is MDM (Mobile Device Management) implemented on the device?

- Yes
- No

Compliance Response

Please refer to CJIS Security Policy v5.8 Section 5.13.2.

2). Do you check the mobile devices to ensure that no unauthorized changes have been made to them such as the device being rooted or jailbroken?

- Yes

- No

Compliance Response

Please refer to CJIS Security Policy v5.8 Section 5.13.2 Paragraph 3.

3). If the device is capable of running LEADS queries is Advanced Authentication implemented?

*** Answer N/A if the device is NOT capable of accessing LEADS, and is only used to access local RMS, other similar systems, or email.**

***If the device IS capable of running LEADS queries, Advanced Authentication is required and you should answer YES or NO.**

Advanced Authentication (or 2-Factor Authentication) requires additional information, for example a temporary PIN, bio-metric data, or a security certificate to name a few.

In addition, for bio-metric data such as fingerprint to be compliant it needs to be maintained by the agency.

Having a user ID/password for the device, and another user ID/password to access CJ data is not sufficient.

» (Choose One Answer Only)

- Yes
- No
- N/A

Compliance Response

Please refer to CJIS Security Policy v5.8 Section 5.6.2.2.