Security Awareness Training FAQ

To better serve Criminal Justice Agencies with CJIS Security Policy compliance, the Illinois State Police purchased the product CJIS Online. CJIS Online is accessed via the Internet and delivers Security Awareness Training for those criminal justice employees who are around criminal justice information without an escort. Criminal Justice employees who are LEADS certified will have their security awareness training delivered to them during the LEADS certification process. This page of Frequently Asked Questions applies to those employees (IT, Janitorial, Maintenance, Private Contractors) who are required to obtain security awareness training, but who are not required to be LEADS certified.

1. Q) What is Security Awareness Training?

   A) Security Awareness Training provides training on topics from basic data security concepts to advanced data security concepts depending on your role in the organization and your role with criminal justice information. This training is mandated by the Criminal Justice Information Services (CJIS) Security Policy developed by the CJIS Advisory Policy Board (APB) and adopted by the FBI. When finished with security awareness training, the student should have a competent understanding of how to handle criminal justice information in relation to the student's role within their department.

2. Q) Who has to take Security Awareness Training?

   A) Anybody who has unescorted access to criminal justice information must be security awareness trained. Users of the LEADS system are provided security awareness training within their LEADS certification courses. Those who need only security awareness training are employees such as Janitorial, Maintenance, Support, and Information Technology Personnel.

3. Q) What are the different levels of Security Awareness Training?

   A) There are 4 levels of Security Awareness training and each level builds on itself.

   Level 1 (All Personnel who have unescorted access to a physically secure area)
   1. Individual responsibilities and expected behavior with regard to being in the vicinity of criminal justice information usage and/or terminals.
   2. Implications of noncompliance.
   3. Incident response (Identify points of contact and individual actions)
   4. Visitor control and physical access to spaces - discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity.

   Level 2 (All authorized personnel with access to criminal justice information)
   1. All items in Level 1
   2. Media protection.
   3. Protect information subject to confidentiality concerns - hardcopy through

destruction.
4. Proper handling and marking of criminal justice information.
5. Threats, vulnerabilities, and risks associated with handling of criminal justice information.
6. Social engineering.
7. Dissemination and destruction

Level 3 (All authorized personnel with both physical and logical access to criminal justice information)
1. All items in Level 1 & Level 2.
2. Rules that describe responsibilities and expected behavior with regard to information system usage.
3. Password usage and management.
4. Protection from viruses, worms, Trojan horses, and other malicious code.
5. Unknown email/attachments.
6. Web usage.
7. Spam.
8. Physical Security.
9. Handheld device security issues.
10. Use of encryption and the transmission of sensitive/confidential information over the Internet.
11. Laptop security.
12. Personally, owned equipment and software.
13. Access control issues.
14. Individual accountability.
15. Use of acknowledgment statements.
16. Desktop security.
17. Protect information subject to confidentiality concerns.
18. Threats, vulnerabilities, and risks associated with access CJIS Service systems and services.

Level 4 (Personnel with Information Technology roles)
1. All of Level 1, Level 2, and Level 3
2. Protection from viruses, worms, Trojan horses, and other malicious code.
3. Data backup and storage.
4. Timely application of system patches.
5. Access control measures.
6. Network infrastructure protection measures.

4. Q) Where can I take Security Awareness Training?

A) There are two methods available for accessing Security Awareness Training.

1) Open your Internet browser and type the following into the address bar: cjisonline.com

2) Open your Internet browser and type the following into the address bar: https://illinois.cjisapps.com/launchpad/, then click on CJIS Links and click on CJIS Online

Method 1 is a direct connection to CJIS Online, while method 2 gives you access through our new CJIS Portal. Please note that if you're using method 2, then the "IL" must be in uppercase and the word "launchpad “must be in lowercase.

5. Q) I'm on CJIS Online, but how do I get to my training?

   A) Once you are at the CJIS Online Main Menu, you will get to your training in one of two ways:

   1) If you are NOT a private contractor, the you will access your training by clicking on the IT & Agency Users option.

   2) If you are a contractor for a Criminal Justice Agency, then you will access your training by clicking on Vendor Access.

6. Q) What are my CJIS Online User ID and Password?

   A) Please contact your LEADS/Terminal Agency Coordinator (LAC/TAC). The LAC for each LEADS agency has the ability to manage users within the CJIS Online system, including setting up User IDs and Passwords.

7. Q) Is there any training available for CJIS Online?

   A) Yes. There are several short training videos available for CJIS Online that are accessible through our CJIS Portal. Open your browser and go to https://www.cjisportal.com/IL/launchpad and click on the menu option for CJIS Training. In the CJIS Training option you will find a link to CJIS Online training.

8. Q) Do I have to use CJIS Online for my Security Awareness Training?

   A) CJIS Online is the recommended method for obtaining Security Awareness Training provided by the Illinois State Police. CJIS Online provides each agency with an electronic method to deliver and efficiently track Security Awareness Training for staff, contract actors and Non-Criminal Jusitce Agency computer service providers.

   The ISP, however, does recognize that there are instances when the online method of delivering Security Awareness training is not practical, specifically when it comes to the Level 1 training. Therefore, the ISP has developed a paper-training method for Level 1 Security Awareness Training, and a paper confirmation sheet for the employee to sign and for your agency to maintain in your files. You may find the Level 1 Security Awareness training, and the confirmation page in the Audit and Training section of the LEADS 2000 site. Or you may click here for the Level 1 training, and here for the confirmation page.

9. Q) Do I have to pass a test to be properly trained in Security Awareness?

   A) CJIS Online does have a 25 question test you will need to complete and pass in order to be considered Security Awareness trained. Your training records within CJIS Online will not reflect a successful training until the test has been satisfactorily completed.