CJIS Online Training Supplement
For Noncriminal Justice Agencies

This training supplement is intended to assist agencies with questions that may arise when their users view the standard online *Security Awareness Training* at CJISonline.com. The CJIS online training was initially drafted to provide a standard level of basic security awareness training to the widest possible audience. Noncriminal justice agency personnel may experience some confusion when reviewing the information originally drafted for criminal justice agencies and criminal justice contractors. This supplement is intended to alleviate any confusion about the variations in requirements between criminal justice and noncriminal justice agencies.

To view the standard online ***CJIS Security Training*** required for all agency Authorized Personnel:

1. Type www.CJISOnline.com into your web browser's address bar. Hit enter.

2. You should be at the CJIS Online home page which says, "**Welcome to CJIS Online**".

3. Your Agency Security Contact (ASC) should have issued you a username and password to log into the website. Contact the ASC for this information. Do not contact the Arizona Department of Public Safety for this information.

    a. Enter your individual email address or username and password or the generic username and password. Click Login.
    b. You will be prompted to reset your password (unless you are using a generic login provided by your ASC).
    c. You will be at the User Profile page. Review your information. If you do not need to make any changes click the "Everything looks good, let's go to the Dashboard" link at the bottom. If you do make changes click Save.
    d. You will then go through a short tutorial explaining the features of the Dashboard. Click Done when finished.

4. Click the "**Training**" button.
    a. Select Security Awareness. It should say "Your assigned training level is Level 4 CJIS Security Training." If it says anything else, contact your ASC and have them assign you to this level before proceeding.
    b. At the Security Awareness Certification screen there are two sections: Training and Test. You will ONLY take the Training. Do NOT take the test. The test is not required.
    c. Click the Begin Interactive Training button. Your ASC will advise you which sections of the training you need to take. Not all sections apply. Typically, most agencies only need to read the following sections:
        i. Section 1 Welcome
        ii. Section 2 Criminal Justice Information
        iii. Section 4 Information Technology Security
        iv. Section 5 System Access
        v. Section 6 Physical Security
        vi. Section 7 Security Incidents

Agencies that store criminal history electronically will, in addition, need to read the

following sections:

i. Section 8 Passwords & Authentication
ii. Section 9 Advanced Authentication
iii. Section 10 Network Security

d. As you view the training, read the corresponding section noted on the following pages of this training supplement for further explanation for noncriminal justice agencies.

6. Once you have completed the training, no further action is required if you are using an individual login and password. If you are using a generic login and password, you will need to notify your ASC that your training is complete. Your ASC will need to note your training date on the Training Documentation Form. Repeat training is required every two years.

CJIS Online Training Supplement for Noncriminal Justice Agencies

The menu on the left side of the website lists 11 sections of training. Noncriminal Justice Agency Authorized Personnel must view all parts of Sections 1, 2, 4, 5, 6, and 7. Agencies storing criminal history electronically must also read sections 8, 9 and 10.

Section 1.1 Welcome / Section 1.2 Purpose

All agencies which receive criminal justice information (CJI) and/or criminal history record information (CHRI) are required to train all personnel who will have direct or indirect access to CJI/CHRI. Direct access means personnel who access the CJIS system through a computer terminal; indirect access includes personnel who are authorized to view CHRI printouts that are sent to the agency as a result of a fingerprint criminal history check. All authorized personnel must complete the standard CJIS Online Security Awareness training within six months of hire or appointment to a position which allows access to CJI/CHRI; training must be repeated every two years. Authorized personnel include anyone who may have reason to access, view, handle, disseminate, and/or destroy criminal history, including administrative assistants and IT personnel who may only have occasion to view CJI/CHRI incidentally in the performance of their duties.

The Agency Security Contact will ensure training occurs as required and maintain training documentation on all personnel on the agency's Authorized Personnel List. Training records are checked against the Authorized Personnel List when the agency is audited by the Arizona Department of Public Safety Access Integrity Unit.

Section 2.1 What is CJI?

CJI is criminal justice information. Criminal history record information (CHRI) is a part of criminal justice information. CJI would include wanted persons warrants and sex offender registration information.

Section 2.2 What is CHRI?

CHRI from criminal justice information systems (CJIS) may contain some information that is also available through public records, but information from these systems and databases is not public record. All the information from the CJIS must be treated as protected, sensitive information. CHRI contains arrest-based data and information that stems from arrest records.

Section 2.3 Understanding CJIS

There are national and state CJIS systems. FBI CJI data comes from the national CJIS system; each state maintains its own CJI for that particular state and shares certain information with the national system. Some noncriminal justice agencies in Arizona are only eligible for information from the Arizona state system and do not qualify for access to FBI data. Public school districts, charter schools, and government agencies are among those which qualify to receive both national and state CHRI.

The state CJIS Systems Agency (Arizona DPS) is responsible for compliance with the FBI CJIS Security Policy and for offering training to agencies which receive CHRI in order to ensure agencies properly handle and protect the information.

CJIS Online Training Supplement for Noncriminal Justice Agencies

Section 2.4 The Interstate Information Index/Section 2.5 Using CJI

III information is comprised of criminal history record information (CHRI). CHRI is provided to agencies for noncriminal justice purposes such as employment, volunteers, licensees, etc. when fingerprints are submitted. All CJI/CHRI must be safeguarded against unauthorized access. Noncriminal justice agencies must appoint Authorized Personnel and have policies/procedures in place to prevent unauthorized access and dissemination.

Section 2.6 Restricted Data

Most noncriminal fingerprint submitting agencies are not authorized to receive restricted files in their returns. Any criminal history contained in those files that meet noncriminal justice dissemination criteria would be released to the agency as part of the criminal history record information it was entitled to see. FBI CHRI can be accessed for criminal history checks under a specific legal authorization, but FBI CJI restricted files are for criminal justice use only.

Section 2.7 Authorized Purposes

In general, criminal justice purposes apply to law enforcement, apprehension and trial of criminals, and correction/rehabilitation of offenders. Examples of noncriminal justice purposes are employment, volunteers, licensing, adoption, etc. As a noncriminal justice agency, your agency's use of criminal history record information is restricted to the particular purpose for which the fingerprints were submitted that is contained in the statute, ordinance, or executive order that authorizes the fingerprint submittal.

Section 2.8 Authorized Uses

Agencies which receive CJI/CHRI from fingerprint submittals for noncriminal justice purposes are restricted to using the information only for the specific purpose for which it was requested and may not share that information with any person or agency unless specifically authorized by law to share the information.

The online example mentions a purpose code. Agencies which directly access the CJIS computers for their criminal justice purposes have to use particular purpose codes related to their reason for checking the criminal history record information on a particular person. Agencies which submit fingerprints for their indirect access do not have purpose codes; instead, these agencies must write their authorization on the fingerprint card in the "Reason Fingerprinted" box. The type of access an agency is allowed to have depends on the agency's function and what is allowed for the type of agency under law.

A noncriminal justice example would be:
John Doe applies for a non-certified job at a public school and a criminal history check is performed. Later, John Doe applies as a volunteer with a non-profit at-risk youth program. The at-risk youth program must perform a criminal history check under its authorization; the school CANNOT share its criminal history check with the youth program.

2.9 Tips for Handling CJI

There are some differences in what criminal justice agencies are allowed to do with CJI/CHRI and what can be done with it for noncriminal justice purposes. Agencies must develop internal policies and procedures regarding handling and security of CJI/CHRI. Noncriminal justice agencies must train all Authorized Personnel on internal CJI/CHRI handling policies/procedures; training logs are maintained locally at the agency by the Agency Security Contact.

Need to Know CJI/CHRI can only be shared among the agency's Authorized Personnel. Anyone who needs to know about the information or may have occasion to view or handle the information must be on the agency's Authorized Personnel List. Information cannot be shared with friends, family members, or on social media.

Sharing Data Sharing CJI/CHRI for any reason other than the specific authorized purpose. Sharing CJI/CHRI with anyone not authorized to have it is not allowed and is a criminal offense (Arizona Revised Statutes 41-1756). Sharing/disseminating information is only allowed as part of the user's duties on a need-to-know, right-to-know basis under legal authorization that is consistent with the specific purpose for which it was requested.

Personal Use CJI/CHRI may never be requested or accessed for personal use.

Phone/Radio CJI/CHRI obtained for noncriminal justice purposes would not be considered an emergency public safety situation. Information should never be texted.

Faxing Generally, when CJI/CHRI is requested for noncriminal justice purposes, the CJI/CHRI is sent directly to the agency unit which requested it and the information must be secured at the recipient point. CJI/CHRI can only be faxed when authorized and consistent with the purpose for which it was requested.

- Secondary dissemination of CJI/CHRI from one agency to another agency must be specifically authorized by law. If authorized, then the sending agency must log the dissemination according to dissemination rules and verify that the receiving agency is authorized and secure. Having an access ORI/OCA does not constitute authorization under noncriminal justice rules. (Example: School District A and Non-profit B both have access OCAs, but CJI/CHRI on Jenny Doe may not be disseminated from School District A to Non-profit B.)

- Secondary dissemination within an agency from one unit to another is generally allowed as long as the dissemination occurs for the same purpose for which the CJI/CHRI was requested. For example, CJI/CHRI is requested to determine if an individual is qualified for a particular license, and the license is denied. The person appeals the denial, and the appeals process in that agency requires the information to be sent to the agency's review board. The CJI/CHRI can be sent from the licensing unit to the review board because it is the same agency using the information for the same suitability determination.

Section 2.10 Electronic Media

Digital media is so prevalent that all personnel must be trained regarding proper handling of digital media containing CHRI. Digital media containing CHRI should be completely destroyed; it should also be overwritten multiple times prior to the destruction. If your agency electronically stores CHRI, you must have technical safeguards as well as physical safeguards to protect the information, and Authorized Personnel will also need to review additional sections of the CJIS Online Training.

Section 2.11 Hard Copies

Noncriminal justice agencies which submit fingerprints for criminal history record checks receive hard copy results from DPS. Only Authorized Personnel can view or handle these printouts; the CJI/CHRI information must be physically destroyed by shredding or burning when it is no longer needed. There is no set retention period for CJI/CHRI; retention depends on the individual agency's regulations that may govern how long an agency must retain such records, but when regulations are satisfied and the suitability determination is finished, CHRI should be destroyed.

Section 2.12 Physically Secure Locations

The requirements for physically secure locations are set out in the FBI CJIS Security Policy. Criminal justice agencies maintain controlled areas which meet the requirements of a physically secure location; in these cases, anyone with access to the physically secure area, even other agency employees, must either be escorted by an authorized person or have been fingerprinted and trained in CJI/CHRI privacy and security. Most noncriminal justice agencies do not meet the definition of a physically secure location and therefore must designate and establish secure areas as defined in the next section "Physically Unsecured Locations"; noncriminal justice agencies typically do not have a "security perimeter" as described.

Section 2.13 Physically Unsecured Locations

Most noncriminal justice agencies meet this definition. The agency is responsible for establishing processes to provide for physical security of the CJI/CHRI it receives. Visitors to the secure area must be escorted; anyone with unsupervised access to the secure area must be on the Authorized Personnel List.

Section 2.14 Agency Requirements

These requirements apply to both criminal justice agencies and noncriminal justice agencies which handle criminal history record information.

Section 2.15 Impact of Misuse

Misuse of CJI/CHRI (unauthorized use, access, handling, release, dissemination) carries criminal and civil sanctions; offenders may be prosecuted and/or have their employment terminated. Each noncriminal justice agency is required to establish disciplinary policies/procedures that outlines steps to be taken in the event of misuse of CJI/CHRI.

Section 6.1 Physical Security / Section 6.2 Physical Security Responsibilities / Section 6.3 Cellular Device Security

These sections discuss physical security both for hard copy CJI/CHRI and for electronic devices if the agency deals with digital CJI/CHRI either through direct electronic access or by scanning hard copies of CJI/CHRI into a computer database. This information is part of the required training for all personnel; review these sections even if your agency does not utilize a digital access or storage method.

Section 7.1 Security Incident Definition / Section 7.2 Security Incident Policy / Section 7.3 Security Incident Report

This information is primarily for agencies which have digital storage of CJI/CHRI or have a direct or interface access with the CJIS System. System incidents are reportable to the state Information Security Officer if the agency has any form of computer access to the actual CJIS system. This information is part of the required training for all personnel; please review these sections even if your agency does not utilize a digital access or storage method. Your agency should have a reporting system for *any* type of security breach involving CJI/CHRI, not just for compromised electronic security.

If CJI/CHRI is stored or accessed electronically:

- Each user must have a unique password subject to specific requirements that must be changed at least every 90 days.
- Users must log off the system at the end of shift or when finished; accounts cannot be shared by multiple users.
- All users, not just IT administrators should be alert for indicators that the system has been compromised; indicators may include odd changes/modifications in files, new files/user accounts with strange names, accounting discrepancies, mysterious unexplained system crashes, and sudden increases/unusual fluctuations in account activity. Sometimes these indicators may be the only clue that a system's security has been breached.
- All users should know how to report when the system's security appears to be compromised; agencies must have written system security response and handling policies/procedures.

Training Requirements

Once you have viewed all of Sections 1, 2, 4, 5, 6 and 7, you have completed the basic Security Awareness online training component.

The second part of the required training for Authorized Personnel is to complete your agency's Privacy & Security training which should provide you with information regarding how the basic security guidelines are implemented at your agency.

Once you have completed both sets of training, you need to sign the Acknowledgement Statement; if you do not have one, one should be available from your agency's Agency Security Contact (ASC). The ASC also needs to log your training on the Training Documentation form. Training must be repeated at least every two years.