# CJIS considerations for CAD Integration

## CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)

The Criminal Justice Information Services (CJIS) division of the Federal Bureau of Investigation (FBI) was created to provide law enforcement, national security, and intelligence community partners with the necessary criminal justice information they need to protect the public.

CJIS is the largest division of the FBI, and comprises several departments, including the National Crime Information Center (NCIC), Integrated Automated Fingerprint Identification System (IAFIS) and the National Instant Criminal Background Check System (NICS). CJIS monitors criminal activities in local and international communities using analytics and statistics provided by law enforcement agencies.

The database maintained by CJIS provide a centralized source of information and is one of the world's largest repositories of criminal history records and fingerprints. The records are available to law enforcement agencies and contractors around the United States that comply with the CJIS Security policy rules.

## CJI DATABASE

Criminal justice and law enforcement agencies from the local, state and federal levels access the CJIS database for information necessary to perform background checks and track criminal activity. The records are available to law enforcement agencies and contractors around the country that comply with security rules, which include requirements that all data be encrypted and that anyone who accesses the database pass FBI background checks. The security of CJIS data essential.

### Primary Services of the CJI Database

- *Archived fingerprint cards*
  The repository maintains all fingerprint cards submitted by criminal justice and non-criminal justice agencies in its archive as digital jpeg images of all submitted evidence of arrest and CJIS source documentation.

- *Positive identification of offenders*
  The backbone of CJIS is the computerized link between a reportable event and an individual's fingerprints submitted by criminal justice agencies.

- *Criminal history records checks for non-criminal justice purposes*
  Authorized background checks of criminal history record information are provided by CJIS for employment and licensing decisions. These checks are performed for

individuals in many fields, including childcare, public safety and security, mortgage banking, elder/child care and adoptions.

- *Expungement*
  Upon petition by an individual under the Criminal Procedure Article, 10-101—10-109, a court may order the elimination of certain conviction or non-conviction data from an individual's criminal history record. The CJIS implements the court order of expungement and assists other agencies to keep their records accurate.

- *Central registry of sex offenders*
  DPSCS is required to maintain a central registry of sex offender registrants pursuant to the Criminal Procedure Article, 11701—11-721. Criminal Justice officials obtain registration statements from the registrants and forward them to the Sex Offender Registry Unit. Information about registered offenders along with photographs can be viewed.

**CJIS SECURITY POLICY**

The CJIS Security Policy document contains security guidelines, compliance requirements, and agreements for criminal justice and law enforcement agencies to protect the transmission, sources, generation and storage of criminal justice information. A section of the policy states "data are to be protected from unauthorized access whether at rest or in motion. This policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information." Background checks are mandatory for individuals accessing the data.

CJI security requirements apply to every individual including private entities, contractors, employees of a criminal justice entity or non-criminal justice agency representatives with access to, or who operate in support of, criminal justice services and information. The basic premise of the CJIS Security Policy is to provide full support to protect the full lifecycle of criminal justice data. The security policy provides guidance for the creation, viewing, modifying, transmitting, disseminating, storing as well as the destruction of the data.

The policy integrates the presidential directives, FBI directives, federal laws, APB decisions along with guidance from the National Institute of Standards and Technology. The security policy helps to strengthen the partnership between CJIS Systems Agencies and the FBI.

*From the Executive Summary of the **CJIS Security Policy document (CJISD-ITS-DOC-08140-5.6, June 5, 2017)**:*

*"Law enforcement needs timely and secure access to services that provide data wherever and whenever for stopping and reducing crime. In response to these needs, the Advisory Policy Board (APB) recommended to the Federal Bureau of Investigation (FBI) that the Criminal Justice Information Services (CJIS) Division authorize the expansion of the existing security management structure in 1998. Administered through a shared management philosophy, the CJIS Security Policy contains information security requirements, guidelines, and agreements reflecting the will of law enforcement and criminal justice agencies for protecting the sources, transmission, storage, and generation of Criminal Justice Information (CJI). The Federal Information Security Management Act of 2002 provides further legal basis for the APB approved management, operational, and technical security requirements mandated to protect CJI and by extension the hardware, software and infrastructure required to enable the services provided by the criminal justice community. "*

*"The CJIS Security Policy integrates presidential directives, federal laws, FBI directives and the criminal justice community's APB decisions along with nationally recognized guidance from the National Institute of Standards and Technology. The Policy is presented at both strategic and tactical levels and is periodically updated to reflect the security requirements of evolving business models. The Policy features modular sections enabling more frequent updates to address emerging threats and new security measures. The provided security criteria assists agencies with designing and implementing systems to meet a uniform level of risk and security protection while enabling agencies the latitude to institute more stringent security requirements and controls based on their business model and local needs.*

*The CJIS Security Policy strengthens the partnership between the FBI and CJIS Systems Agencies (CSA), including, in those states with separate authorities, the State Identification Bureaus (SIB). Further, as use of criminal history record information for noncriminal justice purposes continues to expand, the CJIS Security Policy becomes increasingly important in guiding the National Crime Prevention and Privacy Compact Council and State Compact Officers in the secure exchange of criminal justice records.*

*The Policy describes the vision and captures the security concepts that set the policies, protections, roles, and responsibilities with minimal impact from changes in technology. The Policy empowers CSAs with the insight and ability to tune their security programs according to their risks, needs, budgets, and resource constraints while remaining compliant with the baseline level of security set forth in this Policy. The CJIS Security Policy provides a secure framework of laws, standards, and elements of published and vetted policies for accomplishing the mission across the broad spectrum of the criminal justice and noncriminal justice communities."*

## CJIS COMPLIANCE

Any access to computer media/systems which contain criminal history record information and other sensitive criminal justice information is subject to the CJIS Security Policy, specifically the Security Addendum (SA) documentation. The purpose of the SA is to provide adequate security for criminal justice systems and information while under the management or control of a private entity or contractor. The SA strictly limits the authorized access to criminal history record information, limits the use of the information to the specific purposes for which it is being provided, and ensures the security and confidentiality of the information consistent with applicable laws and regulations.

CJIS Security Policy allows for agencies to tune their security programs according to their risks, needs, and budget constraints while remaining compliant with the baseline level of security set forth in this Policy. However, protecting CJIS data has become more complicated with the proliferation of the Internet, the cloud, and the growing rate and sophistication of cyber security threats. Because of this growing concern, CJIS developed a set of security compliance standards for organizations, cloud vendors, local agencies and corporate networks. The policies set forth by CJIS cover best practices in wireless networking, remote access, data encryption and multiple authentication. Some basic rules include:

- A limit of 5 unsuccessful login attempts by a user accessing CJIS
- Event logging various login activities, including password changes
- Weekly audit reviews
- Active account management moderation
- Session lock after 30 minutes of inactivity
- Access restriction based on physical location, job assignment, time of day, and network address

The policies set forth by CJIS cover best practices in wireless networking, remote access, data encryption, and authentication. According to CJIS Security Policy, “A physically secure location is a facility, a criminal justice conveyance, or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems”. Building and maintaining a physically secure location requires law enforcement agencies to implement safeguards such as:

- Separating the location from non-secure locations via security perimeters and controls
- Issuing credentials for and maintaining lists of all personnel with location access
- Limiting access to any devices (phones, computers, tablets) capable of displaying CJI
- Controlling physical access to distribution and transmission lines within the location

As important as establishing a physically secure location is facilitating CJIS compliant communications between two separate physical facilities. CJIS policy dictates that anytime "CJI is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via [encryption]". This means that even if an agency establishes secure CJIS control rooms on separate floors of the same building, an additional system to perform encrypted email and file exchanges between locations is necessary.

## Cloud Services

CJIS requirements requires cloud service providers to identify all system, database, security and network administrators who have access to the criminal justice system.

- **Amazon Cloud Services (AWS)**

  AWS services support customer CJIS requirements by addressing the CJIS Security Policy Areas. AWS advertises advanced security services such as:

  - Active logging (AWS CloudTrail)
  - Encryption of data in motion and at rest (AmazonS3's Server-Side Encryption with the option to bring a client key)
  - Comprehensive key management and protection (AWS Key Management Service and CloudHSM)
  - Integrated permission management (IAM federated identity management, multi factor)
  - AWS infrastructure and services have been reviewed by several state and federal law enforcement agencies for conformance.

- **Microsoft**

  Microsoft has commitment to meeting the applicable CJIS regulatory controls allows Criminal Justice organizations to implement cloud based solutions and be compliant with CJIS Security Policy V5.6.

  Microsoft has signed the required CJIS Security Addendum in 34 states. (Alabama, Alaska, Arkansas, Arizona, California, Colorado, Florida, Georgia, Hawaii, Illinois, Indiana, Iowa, Kansas, Kentucky, Maine, Massachusetts, Michigan, Minnesota, Missouri, Montana, New Jersey, New York, Nevada, North Carolina, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, Utah, Vermont, Virginia, and Washington). This listing is current as of 07/01/2018.

## End-to-End Data Protection Services

There are several companies that provide services to state and local government for data encryption, secure e-mail, and CJIS compliance. One company, Virtru, has a comprehensive description of some of the hurdles.

- *The CJIS Advanced Authentication Requirement*
  *FBI Security Policy section 5.6.2.2.1, or the Advanced Authentication Requirement, compels agencies to use multi-factor authentication when accessing CJI. A quick example of multi-factor authentication is your debit card. While shopping with your credit card (in the U.S., at least) requires only what you have (the number on your credit card), your debit card also requires something you know (your PIN). If a thief steals your debit card, they can't use it until they also get your PIN. One common type of multi-factor authentication involves a software application or physical device that generates a unique, one-time password at timed intervals. This wildcard password (what you have) adds a second level of complexity to your password (what you know), providing multiple barriers of entry to potential data thieves.*

- *CJIS Compliance and Data Encryption*
  *The CJIS has also established requirements for the use of data encryption when storing and using sensitive data, as well as including CJI in communications. A minimum of 128 bit encryption is required, and keys used to decrypt data must be adequately complex (at least 10 characters long, a mix of upper and lowercase letters, numbers and special characters) and changed as soon as authorized personnel no longer need access. Like multi-factor authentication, data encryption adds an extra layer of security to your data — if a criminal gains access to an encrypted file or communication, that information is useless without the key to decrypt it. Email presents its own CJIS compliance challenges. A tremendous amount of criminal justice information is exchanged via email and standard email services do not offer the encryption required by CJIS. Most third-party encryption services are either difficult to use, expensive, or both. Many also require senders or receivers to establish new accounts to view CJIS-compliant emails.*

- *Personnel and Training Considerations*
  *Knowing what your agency needs to maintain CJIS compliance is one thing, but putting it into practice is another. It's critical that you provide frequent staff training on CJIS best practices, make sure there's ample documentation and knowledge sharing and implement agency-wide security protocols and password requirements.*

  *Organizations can hire IT consultants, devote a department strictly for CJIS compliance and build the necessary infrastructure required to support the official policies. Alternatively, they can outsource their data protection services to companies that specialize in CJIS compliance. This is a great long-term solution for agencies and contractors that want to streamline their CJIS compliance efforts without making huge investments in staffing and infrastructure.*

## UTILIZING CAD-CAD STANDARDS

CAD systems require real time delivery of data to be an effective incident/emergency management tool. During CAD operations, data from the CJIS may be copied, pasted and/or attached as part of the call history and incident information. However minimal guidance for CAD-Traffic Operations Center (TOC) integration and CJIS compliance has been published to date.

A set of standards for CAD-CAD integration that has currently been developed can be used as a reference for CAD-TOC. The IJIS Institute, comprised of over 400 member companies and individual associates from government, nonprofit, and educational institutions from across the United States, is a good source of information. Founded in 2001 as a 501(c)(3) nonprofit corporation with national headquarters on The George Washington University Virginia Science and Technology Campus, the IJIS Public Safety Technology Standards Committee has developed a document **CAD-to-CAD Data Sharing (A Review of Recommended Standards) dated February, 2017.**

The following information is taken from the document.

*In addition, to the encryption of the communications path, CAD-to-CAD middleware products must assume the presence of CJI data in incident data and apply appropriate CJIS Security Policy for the storage and tracking of the incident data for the longevity of the incident within middleware environment. If a CAD-to-CAD middleware is not being used, the assumption (e.g., exchange policy) is that the receiving CAD entity will handle CJIS CJI marked data in accordance with the CJIS policy. When dealing with a non-law enforcement CAD system, such as a Department of Transportation (DOT) system, CJI data, such as personal information, needs to be identified in the incident history, such that the CAD-to-CAD middleware/interface can appropriately redact the CJI information. The CAD-to-CAD governance agreement must cover what type of CAD incidents and information can be transferred to non-Law Enforcement systems. If there is no use of FBI CJIS data within the system, then the CJIS Security Policy would not apply.*

- The CAD-to-CAD communications must be fully encrypted end-to-end and function in a shared network environment and provide CJIS compliance.
- The CAD-to-CAD middleware must provide continuity and comply with CJIS security for storage of the CAD call history.
- If a non-Law Enforcement system requires access to CAD call histories then, the CAD-to-CAD middleware must redact and encrypted the CAD call information to be CJIS compliant.
- If the CAD-to-CAD middleware provides remote access, *e.g.*, web or in-vehicle, into the application. The remote access must comply with CJIS Security Policy standards.

Other applicable items are described in this document.

- *Firewall*
  Networks requiring access to CJIS applications must be protected by firewall devices configured explicitly to allow only permissible protocols and traffic inherent in the networked environment. Configuration must provide a point of defense with controlled access from both inside and outside the CJIS network. The device must provide logging capability and audit capability.

- *Anti-Virus Program*
  All servers and workstations must be protected by a comprehensive Anti-Virus program. The Anti-Virus software must be configured to receive automatic virus pattern updates. Virus scanning must be configured to execute scanning processes without user intervention.

- *Patch Management Process*
  All servers and workstations must be protected by a patch management program. Servers and workstations must be enabled to receive distributed operating system upgrades, patches and hotfixes without user intervention. All updates must be certified in a test environment prior to distribution.

- *Operating System*
  Only servers and workstations with operating systems having a current support commitment by the manufacturer will be allowed to reside within a CJIS network. (Note: Microsoft is a complaint system.)

- *Multiple Browser Sessions*
  Concurrent browser sessions open to internet sites while accessing any CJIS application are strictly prohibited.

- Intrusion Detection
  All CJIS network environments should be protected by an intrusion detection system. Such systems examine information from a number of system and network sources then analyze the information for signs of intrusion (attacks aimed at the organization) and misuse. All servers residing inside a CJIS subnet should be protected by host intrusion detection software.

**FINAL THOUGHTS**

Currently minimal guidance has been published to address CJIS compliance with CAD-to-Traffic Operations Center integration. CAD-TOC could be in the form of a direct, (typically redacted) API feed from the CAD system to the TOC or through middleware that ensures CJIS compliance.

Both the CJIS Security policies as well as recently developed standards for CAD-to-CAD can be considered for CAD-TOC integration as described below. These guidelines apply to when DOT and State Police are collocated in the same facility or not.

In summary, CJIS compliance with CAD integration within a TOC environment can be accommodated using the following scenarios.

- Redacted API from the CAD vendor to eliminate CJIS sensitive information
- Un-redacted direct API from the CAD system. TOC operators and other DOT personnel with access to the data would need background checks and meet other applicable CJIS Policy requirements.
- API from middleware. CJIS requirements would be required in the feed from the middleware vendor.

## CAD-TOC Integration Guidelines

| |
|---|
| If CJIS information attached to an incident is transferred directly to a partnering system, the transfer must meet/comply with CJIS Security Policy. |
| If a TOC requires access to CAD call histories, the API can either include redacted information appropriate for CJIS compliance (redaction provided from the CAD software system vendor) or if an un-redacted feed, the TOC would need to comply with CJIS Security Policies. This would include background checks for all employees. |
| If middleware products are used, they must reflect appropriate CJIS Security Policy for the storage and tracking of the incident data for the longevity of the incident within middleware environment. |
| If the middleware provides remote access, *e.g*., web or in-vehicle, into the application, the remote access must comply with CJIS Security Policy standards. |
| Networks requiring access to CJIS applications must be protected by firewall devices configured explicitly to allow only permissible protocols and traffic inherent in the networked environment. The device must provide logging and audit capability. |
| Any two way connections, rather than a simple push from the CAD system, would require full compliance of the CJIS Security Policy for all DOT employees with access. |
| All servers and workstations must be protected by a comprehensive Anti-Virus program. The Anti-Virus software must be configured to receive automatic virus pattern updates. Virus scanning must be configured to execute scanning processes without user intervention. |
| Only servers and workstations with operating systems having a current support commitment by the manufacturer will be allowed to reside within a CJIS network. (Note: Microsoft is a complaint system.) |
| All CJIS network environments should be protected by an intrusion detection system. All servers residing inside a CJIS subnet should be protected by host intrusion detection software. |
| If there is a common data storage between DOT and law enforcement agencies, the storage method must comply with the CJIS Security Policy. If cloud services are used, the provider must be CJIS certified (AWS and Microsoft cloud services are certified examples). |