I-95 CORRIDOR COALITION

CJIS Considerations for CAD Integration

Criminal Justice Information Services (CJIS)

The Criminal Justice Information Services (CJIS) division of the FBI was created to provide our law enforcement, national security, and intelligence community partners with the necessary criminal justice information they need to protect the public. CJIS monitors criminal activities in local and international communities using analytics and statistics provided by law enforcement agencies. The databases 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.

CJIS Security Policy

The CJIS Security Policy (**CJISD-ITS-DOC-08140-5.6, June 5, 2017**) 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." Successful background checks are mandatory.

CJIS Compliance

The 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

Computer Aided Dispatch (CAD) Integration

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.

Currently minimal guidance has been published to address CJIS compliance with CAD-to-Traffic Operations Center integration (TOC). 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.

However, a recent set of standards for CAD-CAD integration developed by the IJIS Institute (**CAD-to-CAD Data Sharing, A Review of Recommended Standards, February, 2017**) can be considered.

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.
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).

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.

I-95 CORRIDOR COALITION

info@i95coalition.org

5000 College Avenue, Suite 2200, College Park, MD, 20742

For more info contact Denise Markow, 301.789.9088