Criminal Justice Information Systems (CJIS) Best Practices Guide and Resources for GIS

MN Geospatial Advisory Council

Authors:
Chair – Britta Maddox, Public Safety Data System (PSDS) Fire Records Management System (RMS) Administrator, MNGAC Member at-large
Co-Chair – Cory Richter, Ramsey County General Supervisor – Highway Maintenance and Construction, MNGAC Chair/Metro Cities Representative

Contributing Subject Matter Experts:
Trish Heitman-Ochs, Woodbury PD Crime Analyst
Matt Goodman, St Louis County GIS
Doug Matzek, Washington County GIS
Karen Haines, Washington County Sheriff's Office (WCSO) Systems Manager
Karie Weldon, WCSO Business Analyst
Linda Curtis, WCSO Business Analyst
Angela Backer-Hines, Eagan Crime Analyst
Garith Sherk, Minnetonka Crime Analyst
Eric Kopras, Woodbury GIS

Consulting Members:
Olivia Anderson, Bureau of Criminal Apprehension (BCA)
Diane Bartell, BCA

Table of Contents

1. INTRODUCTION

Workgroup Mission Statement:

The MN Geospatial Advisory Council recognizes that occasionally non-public safety GIS staff get pulled in for support tasks dealing with secure or sensitive data which may require special considerations. The workgroup therefore sought to provide understanding and definitions of Criminal Justice Information (CJI) and other secure or sensitive data types and provide best practices and resources for access, dissemination, and disclosure of said information.

Document Objectives:

Discern CJIS-compliant (Criminal Justice Information Systems) best practices for sharing data within the GIS community, particularly as it relates to Emergency Management or critical incidents and infrastructure

Share this guide amongst the broader MN GIS community and use these principles to inform future MN GAC projects

Target Audience:

- **GIS professionals –** specifically those tasked with public safety related products/analysis
- **Data practices responsible authority within each agency –** this could include the Terminal Agency Coordinator (TAC), alternate TAC, Local Agency Security Officer (LASO), law enforcement staff who authorize and release response data (typically records staff or office administrators but can also be sworn peace officers).
- **IT staff –** IT staff at each local agency should be versed in the network and physical security rules and have adequate plans in place for ensuring network and physical security even in the event of a critical incident where the establishment of an EOC (Emergency Operations Center) outside of normal physically secure buildings may be required.
- **Emergency Manager –** staff responsible for planning and leading the responses to natural disasters and other emergencies

Glossary of Terms:

- **MN BCA** - The Bureau of Criminal Apprehension (BCA) provides investigative and specialized law enforcement services to prevent and solve crimes in partnership with law enforcement, public safety and criminal justice agencies. Services include criminal justice training and development, forensic laboratory analysis, criminal histories and investigations.[1]
- **Criminal Justice Information (CJI)** - protected under the FBI's Criminal Justice Information Services (CJIS) Division's CJIS Security Policy which discusses authorized use, access, dissemination, and disclosure. See Appendix A for a copy of the CJIS Security Policy.
- **PII: Personally Identifiable Information** – in the scope of CJIS this includes any information that can be used to distinguish and trace and individual's identity. Examples include name, social security number, or other biometric records alone and or in conjunction with information such as DOB, place of birth, mother's maiden name, etc. This information must be extracted from CJI for official business only.
- **Safe at Home Act -** MN Statutes Chapter 5B, "The legislature finds that individuals attempting to escape from actual or threatened domestic violence, sexual assault, or harassment or stalking frequently establish new addresses in order to prevent their assailants or probable assailants from finding them. The purpose of this chapter is to enable state and local agencies to respond to requests for data without disclosing the location of a victim of domestic violence, sexual assault, or harassment or stalking; to enable interagency cooperation with the secretary of state in providing address confidentiality for victims of domestic violence, sexual assault, or harassment or stalking; and to enable program participants to use an address designated by the secretary of state as a substitute mailing address for all purposes."[2]
- **LASO: Local Agency Security Officer –** the liaison between the local agency and the CJIS System Agency Information Security Officer at the BCA. Often, this is the IT director for the local PD or Sheriff's Office. The LASO is responsible for ensuring proper personnel security screening, physical security of data terminals accessing the CJDN or containing CJI, ensuring network compliance with the CJIS Security Policy and documenting procedures for local agency access to CJI.
- **TAC / Assistant TAC: Terminal Agency Coordinator –** local agency POC for CJIS access and compliance with CJIS policies. Often, this is the records supervisor or other office administrator for the local PD or Sheriff's Office.
- **Critical Incidents –** As described by FEMA, "Any natural or man-made event, civil disturbance, or any other occurrence of unusual or severe nature that threatens to cause or causes the loss of life or injury to citizens and/or severe damage to property."[3]
- **Storage requirements for security** – where on the network, who can access, etc, what is 'public accessibility', password requirements/policy for access

[1] https://dps.mn.gov/divisions/bca/about/Pages/default.aspx
[2] https://www.sos.state.mn.us/safe-at-home/about-safe-at-home/
[3] https://training.fema.gov/programs/emischool/el361toolkit/glossary.htm

2. REQUIRED ACCESS STANDARD

These are the standard certifications required for anyone to be able to access criminal justice information (CJI). It should also be noted that access must be for authorized purpose only, as defined by federal statute. Having a background check and training allows access to CJI but only when necessary per statute. Your TAC can advise if your need falls under the appropriate use. A word of caution – training gains you access but we have statutory requirements giving a one-strike rule if there are instances of misuse (particularly DVS access).

A. CJIS Security Awareness Training and Test

- Required for anyone who may have physical or logical access to CJI during the course of their duties – including IT Staff responsible for network security and GIS Staff that may be called in during a critical incident
- This even includes janitorial staff that may stumble upon CJI during other duties
- CJIS Online link provided here
  - For a username and password, please contact your agency's Terminal Agency Coordinator (TAC).
- There are four different levels based on your role's level of interaction with CJI:
  - Level 1 Security Awareness Training 5.2.1.1: Those with physical access only. These individuals are not performing a criminal justice function. They would have incidental access; i.e. janitorial, maintenance, vending machine vendors, etc.
  - Level 2 Security Awareness Training 5.2.1.2: Those with physical access only performing a criminal justice function; i.e. paper shredding, records clerks, scanning services, couriers, etc.
  - Level 3 Security Awareness Training 5.2.1.3: Those with physical and logical access. This access includes the electronic ability to see criminal justice information; i.e. majority of criminal justice staff, terminal operators, officers with MDTs, etc.
  - Level 4 Security Awareness Training 5.2.1.4: All those with an Information Technology role; i.e. system administrators, security administrators, network administrators, etc.
- Certification valid for 2 years and then must be renewed; includes a background check

B. BCA Training

Specialized training courses for those fulfilling certain roles and general overview of data practices and CJDN operations. Registration fees may apply to each class.

- **TAC Workshop:** This one-day course is designed for new and existing Terminal Agency Coordinators (TAC) as a summary of the duties and responsibilities a TAC has with regard to BCA MNJIS and FBI NCIC access. By the conclusion of this

class, students will have the knowledge and skill set for performing TAC functions at their agency.

- **MNJIS Operator:** This two-day course, which combines the MNJIS One-Day Basic Operator course with additional specialized training, is designed for full-access operators who run queries and enter records into the Minnesota and NCIC hot files. Students completing this course will learn the policies and procedures for Criminal Justice Data Communications Network (CJDN) operators. Students will gain an understanding of system security, file queries, criminal history, hot files, and the hit confirmation process. This course covers the content from MNJIS One-Day Basic Operator.

- **LASO Certification** - located within CJIS Online. As the LASO, you are required to complete both the Security Awareness and LASO certifications. Required to be completed yearly

C. Other training/certification/authorization may be necessary based on types of data

3. AUTHORITATIVE SOURCES REGARDING CJI

Recognizing where your authoritative sources of CJI are is the first step. The second step is to be compliant with the policies surrounding those sources. In the State of Minnesota, there are three main access points by which you could be receiving CJI – the FBI CJIS Systems, BCA-provided data, and data covered by MN Chapter 13. The key point is to be aware of the source and aware of the potential that something that is CJI could be in there (ex. RMS systems, court records – depending on what people have submitted, criminal histories, driver's license data coming from CJDN, etc).

If you're following the BCA policy, you're compliant with FBI. The opposite is not always true. CJI can be a part of any of this – it's all dependent on the original source of the data. BCA 5000-2 policy has a list of systems and the data within. If you have access to that system, you should already be in compliance.

A. CJI – Only information coming from FBI CJIS Systems

Covered by CJIS Security Policy – very small scope
See Appendix A

Summary of the CJIS Security Policy – Designed to provide a minimum set of security requirements for creation, viewing, modification, transmission, dissemination, storage, and destruction of FBI-provided Criminal Justice Information (CJI). Agencies may impose stricter controls governing in a risk-based approach.

Section 3 of the CJIS Security Policy covers the roles and responsibilities that fall under each role within an organization when it comes to data security.

Section 4 defines CJI as the "…term used to refer to all of the FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions including but not limited to biometric, identity history, biographic, property, and case/incident history data."[4] Criminal History Record Information (CHRI) is a restricted subset of CJI data which is governed by CFR Title 28, Part 20 (Appendix D). Section 4 continues to discuss the proper access, use, storage, and dissemination of all the defined data that qualifies as CJI. Personally Identifiable Information (PII) is also defined here as that which can be used to distinguish and or trace an individual's identity, which is again protected by policy.

Section 5 describes the policy items and implementation steps of said policies that agencies must address. There are 13 policy areas – Information Exchange Agreements, Security Awareness Training, Incident Response, Auditing and Accountability, Access Control, Identification and Authentication, Configuration Management, Media Protection, Physical Protection, Systems and Communications Protection and Information Integrity, Formal Audits, Personnel Security, and Mobile Devices. These areas are covered in depth within the CJIS Security Policy, along with appendices that provide samples, diagrams, and best practices.

[4] CJIS Security Policy, page 10

NOTE: The BCA's policy encompasses the CJIS Security Policy above with all data elements categorized based on their source. The only real delineation comes when redacting for legal purposes, which should fall outside the scope of anything GIS-related.

- If the source is from FBI, it will be CJI
- If the source is from BCA, it will be FBI CJI and BCA CJI combined
- In short, everything should be treated as FBI CJI regardless of its source, according to the BCA.

B. BCA-provided Data

Covered by CJDN Security policy
See Appendix B

Summary of the CJDN Security Policy – This document is intended to be an extension of the FBI CJIS Security Policy in reference to BCA-provided data, providing specific guidance for meeting CJIS Security requirements. The first portion of the document enumerates the difference between the CJIS System Agency Information Security Officer (CSA ISO), a BCA employee, and the Local Agency Security Officer (LASO). Enforcement and security are also listed here, providing that all agencies be responsible for ensuring appropriate measures are taken. The CJDN policy also provides standards for incident response, should there be a security breach, and a template for response policy, NIST Special Publication 800-61.

Technical security standards make up the bulk of the CJDN security policy including account administration, advanced authentication, application development, BCA systems and data access, camera guidance for body/squad/surveillance cameras, cloud security, audio and video conferencing, employees, vendors and contractors, encryption, digital faxing, firewalls, logging, multifunction devices and printers, radio traffic, soft phones, VPNs, virtualization, vulnerability remediation and system updates, and wireless networks.

One of the main items in the CJDN Security Policy is the encryption requirements. All devices must be FIPS 140-2 compliant with a 128-bit symmetric key to access and or transmit CJI. In addition, when CJDN must be accessed outside of a physically secure location, advanced authentication must be used with the encryption to ensure data security. This is a particularly relevant consideration in times of critical incident management as temporary command posts may be established.

C. MN Chapter 13 and Data from Local Law Enforcement Agencies

See Appendix C

Summary of MN Statute 13.82 COMPREHENSIVE LAW ENFORCEMENT DATA[5]

Disclaimer – there are many nuances to this statute and exceptions enumerated in other related statutes. Below is a basic summation of arrest, call for service, and incident response data and its default dissemination status. This is generally assumed to have been sourced from the local agency and that the data is only Chapter 13 applicable, but consideration must always be given to the source of the data as that could change the dissemination status. The statute itself should be viewed in its entirety prior to dissemination of any CJI and related statutes also consulted, where applicable. Please speak to your county attorney or local prosecutor for nuances and final determination regarding the statute.

Whether or not data is public is partially dependent on its origination – Arrest data, Incident data, or Call for Service data.

Arrest data relates to any actions taken by law enforcement to cite, arrest, incarcerate, or otherwise substantially deprive an adult of liberty and shall be PUBLIC at all times. Booking photos taken at the time of arrest are also considered PUBLIC information. Data from arrest warrants is CONFIDENTIAL until the defendant is taken into custody, served, or appears before the court with exception for when making the information public would serve public interests.

Call for Service data relates to the request by the public for LE services is PUBLIC. The audio recording of a 911 call is PRIVATE except for a written transcript of the recording is PUBLIC, without revealing the identity of the caller.

Incident data is the documentation of law enforcement's response to the request for service as well as their actions taken under their own initiative for public safety and traffic incidents and is inherently PUBLIC.

Incident data regarding the investigation of a crime is deemed CONFIDENTIAL or PROTECTED NONPUBLIC until:

- a decision by the agency or appropriate prosecutorial authority not to pursue the case;
- expiration of the time to bring a charge or file a complaint under the applicable statute of limitations, or 30 years after the commission of the offense, whichever comes earliest; or
- exhaustion of or expiration of all rights of appeal by a person convicted on the basis of the investigative data.

[5] https://www.revisor.mn.gov/statutes/cite/13.82

After one of those clauses occurs, the information becomes PUBLIC upon request, unless the release of data would jeopardize other ongoing investigations and/or would reveal the identity of protected individuals. Any investigative data presented as evidence in court shall be public. A court order can also be obtained during an active investigation to release the contents of an investigation per judge's order. Public data may also be withheld if the agency reasonably believes that public access would endanger the physical safety of an individual or cause a perpetrator to flee, evade detection, and or destroy evidence. Any dispute of this withholding would need to be contested in court.

Reporters and victims of child abuse or neglect and reporters and victims of vulnerable adult maltreatment are always PRIVATE, whether active or inactive. Financial transaction data and account numbers are always PRIVATE NONPUBLIC, regardless of the investigation status. Data uniquely describing lost, stolen, recovered, or confiscated physical property is PRIVATE.

Investigative techniques and other law enforcement processes are considered CONFIDENTIAL provided they are publicly accepted practices under courts of law. However, the use of surveillance technology to capture audio, video, photos, or other electronic recording devises of the general public for purposes of conducting an investigation, responding to an incident or request for service, monitoring or maintaining public order and safety, or engaging in any other law enforcement function authorized by law is PUBLIC data.

This statute allows for discretion by law enforcement entities to make confidential or protected nonpublic data public when it is determined that the access will aid the law enforcement process, promote public safety, or dispel widespread rumor or unrest. There are also provisions for making public data inaccessible when not feasible to separate the public and nonpublic data and or when protecting the identity of certain individuals, as listed in the statute.

4. COMMON TOOLS AND SAMPLE USE CASES

These are only some tools available for use and most can be customized to a department's needs and security level. Below are some examples of available options and a brief synopsis of what that tool provides:

Open source/free mapping tools (Bing, Google, QGIS, etc.) – Review the platform's security standards and consider what data you are submitting to the service to be processed and/or stored in their cloud.

ArcGIS Pro Crime Analysis and Safety Toolbar – Set of crime analysis tools and sample projects that can be added to ArcGIS Pro to support tactical, strategic, and investigative analysis functions. Desktop tool, no CJIS/CJDN security concerns.

ArcGIS Pro Intelligence – A specific iteration of ArcGIS Pro directed at investigative and intelligence professionals. Still includes most of the normal ArcGIS tools, built to streamline intelligence data processing from multiple sources into visualizations (timelines and link charts integrated with maps). Desktop tool, no CJIS/CJDN security concerns.

ArcGIS Online and Story Maps – Online interactive maps and data dashboards for publishing and sharing data, internal or external. CJIS/CJDN security concerns depending on the data used in the applications and if it is stored in Enterprise Portal or ArcGIS Online (ArcGIS Online Cloud pending FedRAMP Moderate certification which is the equivalent of CJIS compliance).

Survey123 – Form-centric data gathering and sharing solution through a Mobile Application using ArcGIS. Shared feature services work hand-in-hand with Field Maps. Best use for collecting form data, such as surveys with pre-defined fields, can capture images, etc. CJIS/CJDN security concerns depending on the data used in the applications and if it is stored in Enterprise Portal or ArcGIS Online.

Field Maps – Map-centric data collection and sharing solution through a Mobile Application on devices with GPS capability to edit and track data through ArcGIS. Could be used to track graffiti, damaged utilities, managing fleet/equipment, etc. CJIS/CJDN security concerns depending on the data used in the applications and if it is stored in Enterprise Portal or ArcGIS Online

ArcGIS Mission – Built for command staff to streamline tactical operations during events, including planning, resource assignment and real-time updates and communication. Desktop and mobile application, track and visualize staff movements and sent information back and forth. Potential for CJIS/CJDN security concerns for officer safety and the data shared in the messaging component.

Drone2Map – Provides real-time or historic drone imagery which can be monitored live or turned into a 3D model of the location. Could be used to prepare for a search warrant, event planning, searching for missing persons, etc. Probably no CJIS/CJDN security concerns.

Transparency Hub/Crime mapping (public) – Pre-built customizable set of online story maps and dashboards supplied by ESRI to share public safety data with the public. CJIS/CJDN security concerns if data released through these tools is not public.

CrimeView Analytics – A map centric application offered from CentralSquare that connects CAD and RMS data systems. Enables the creation of dynamic dashboards composing of custom maps, charts and tables and the ability to automate email alerts and dashboard views.

LexisNexis/Accurint – software itself is already compliant with security policies, based on what the BCA allows us to contribute. Secure access requirements and dissemination rules would apply.

5. GIS DATA SOURCES

Many GIS data sets that are useful for conducting crime analysis are publicly available for download. Below is a list of web resources where you may find some of the basic GIS layers you may need to conduct your work. Please note that care must be taken, following the guidance within this document, Minnesota statutes, and CJIS best practices, to ensure that combining these data with crime incident information does not violate an individual's right privacy (for example, tying a domestic abuse crime record to a parcel owner's name based on location and address).

Minnesota Geospatial Commons - a good place to find geocoding data sets like addressed road centerlines and address points.

Site: https://gisdata.mn.gov/

Minnesota Natural Resources Atlas - clearinghouse for Minnesota data mostly sourced from other entities

Site: https://mnatlas.org/

HIFLD (Homeland Infrastructure Foundation-Level Data) - clearinghouse for critical infrastructure data that is sourced from a wide variety of entities and systems. These data are not always authoritative or current, so it should be reviewed before use, but it is often still considered the 'best available'.

Site: https://hifld-geoplatform.opendata.arcgis.com/ or, accessible via the MN GAC's Critical Infrastructure GIS Data webpage

Esri Living Atlas – data layers available to users within their ArcGIS Online system and include a vast array of curated data sets, including ready-to-use community demographic data, which helps put crime statistics into context.

Site: https://www.arcgis.com/ (requires a user account)

Minnesota NG9-1-1 Data - In support of the state's eventual transition from E9-1-1 to NG9-1-1, stakeholders are working towards aggregated statewide datasets for address points, road centerlines, and emergency services (fire, law, medical, etc.) boundaries. Those involved in this work are hopeful that these data sets can be made publicly available.

Address points, center lines, responder boundaries – statewide coverage

MN BCA Crime Data Explorer – provides summary incident and arrest statistics statewide. Already compliant as it is provided publicly by the BCA. Jurisdiction-based, no latitude/longitude.

Site: https://cde.state.mn.us/

6. APPENDICES

Appendix A: **CJIS Security Policy**

Appendix B: **CJDN Security Policy**

Appendix C: **MN 13.82 Statute**

Appendix D: **CFR Title 28 Part 20**

Additional CJIS Resources