Minnesota Geospatial Advisory Council
Committee/Workgroup Meeting Minutes

CJIS Best Practices and Data Standards Guide for GIS

Meeting date: June 22nd, 2022

Minutes created by: Britta Maddox

Participants:
Chair: Britta Maddox, Business Analyst WCSO and GAC Member
Co-Chair: Cory Richter, Ramsey Co General Supervisor of Highway Maintenance, GAC Chair
Trish Heitman-Ochs, Woodbury PD Crime Analyst
Matt Goodman, St Louis County GIS
Doug Matzek, Washington County GIS
Carey Strouse, Coon Rapids PD Crime Analyst
Karen Haines, WCSO Systems Manager
Karie Weldon, WCSO Business Analyst
Linda Curtis, WCSO Business Analyst
Patti Zafke, BCA
Angela Backer-Hines, Eagan Crime Analyst
Garith Sherk, Minnetonka Crime Analyst
Eric Kopras, Woodbury GIS
Sean Murphy, MetCouncil
Amy Larsen, WCSO Records

Agenda Items:

1. May Action Item Review
    a. Trish - ESRI LE SME's – John Beck and Chris Delaney may have federal rules and guidance

    Chris at ESRI said that they don't have any official documentation to speak of for CJIS data, but current best practice (which they expect to change in 2023) is that any data containing CJI should be served using Enterprise. Since using enterprise keeps everything living within your network, so there really aren't any additional CJIS considerations on the ESRI side other than federating agency log-ins to your existing single-sign on security model- (for most agencies, that is Active Directory). They have lots of agencies who have Enterprise set up, and even a few that have their Enterprise instances on cloud architecture- i.e. Amazon or Azure Gov Cloud. For most LE agencies though, the easiest path is just standing up Enterprise on existing servers within their LE network.

    BUT – he also informed me that ESRI is in the process of being audited for FedRAMP moderate certification for ArcGIS Online. They are anticipating being able to change their terms of service to allow for the storage of PII in ArcGIS Online around the end of March 2023. This relates to CJIS because the NIST standard that is the basis for FedRAMP moderate is identical to CJIS. Long story short, once the initial FedRAMP moderate

certifications is complete, they plan to have their LE user agencies begin to work with their state's authorities to audit the use of ArcGIS Online for CJIS data approval.
https://www.fedramp.gov/
https://www.nist.gov/news-events/news/2018/06/nist-publishing-special-publication-sp-800-171a-assessing-security

SO… Things will change within the next year as to what their recommendations are and what options we would have in LE to use AGOL for PII if we want.

b. Cory – 13.82, BCA Guidelines on data storage
c. Eric/Trish – examples of activities
d. Britta – overall compilation
e. Trish – training necessary based on certain types of data
    i. CJIS Security policy reviewed and NCIC security docs reviewed – anyone who is allowed to work on LE data has to have this in order to work; that's the basis
        1. GIS staff working with this kind of data should have CJIS Security Awareness Test as part of basic staff onboarding (include link/how-to/CJIS LaunchPad through your TAC)

2. Assign action items
    a. Britta – summarize statute
    b. Matt Goodman/Cory – data sources summarization, open source/tenant registry
    c. Britta – CAD/Incident/Arrest differentiation
    d. Trish/Eric – list of example activities
3. Compile above items between now and next meeting – next meeting review rough draft of document, identify portions we missed/etc other information we need/want
4. Adjourn – Wed August 10th at 10a next meeting

4 CRIMINAL JUSTICE INFORMATION AND PERSONALLY IDENTIFIABLE INFORMATION

4.1 Criminal Justice Information (CJI)

Criminal Justice Information is 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. The following categories of CJI describe the various data sets housed by the FBI CJIS architecture:

1. Biometric Data—data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. Used to identify individuals, to include: fingerprints, palm prints, iris scans, and facial recognition data.
2. Identity History Data—textual data that corresponds with an individual's biometric data, providing a history of criminal and/or civil events for the identified individual.
3. Biographic Data—information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.
4. Property Data—information about vehicles and property associated with crime when accompanied by any personally identifiable information (PII).
5. Case/Incident History—information about the history of criminal incidents.

The following type of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g., ORI, NIC, UCN, etc.) when not accompanied by information that reveals CJI or PII.

4.3 Personally Identifiable Information (PII)

For the purposes of this document, PII is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. Any FBI CJIS provided data maintained by an agency, including but not limited to, education, financial transactions, medical history, and criminal or employment history may include PII. A criminal history record for

example inherently contains PII as would a Law Enforcement National Data Exchange (N-DEx) case file.

PII shall be extracted from CJI for the purpose of official business only. Agencies shall develop policies, based on state and local privacy rules, to ensure appropriate controls are applied when handling PII extracted from CJI. Due to the expansive nature of PII, this Policy does not specify auditing, logging, or personnel security requirements associated with the life cycle of PII.

Figure 2 – Dissemination of restricted and non-restricted NCIC data

A citizen of Springfield went to the Springfield Police Department to request whether his new neighbor, who had been acting suspiciously, had an outstanding warrant. The Springfield Police Department ran an NCIC persons inquiry, which produced a response that included a Wanted Person File (non-restricted file) record and a Known or Appropriately Suspected Terrorist File (restricted file) record. The Springfield Police Department advised the citizen of the outstanding warrant, but did not disclose any information concerning the subject being a known or appropriately suspected terrorist.