Best Practices

Leveraging Computer-Aided Dispatch to Enhance Suspicious Activity Reporting

Best Practices Leveraging Computer-Aided Dispatch to Enhance Suspicious Activity Reporting

Table of Contents

This project was supported by Grant No. 2017-D6-BX-0001 awarded by the Bureau of Justice Assistance (BJA), in collaboration with the U.S. Department of Homeland Security (DHS). BJA is a component of the U.S. Department of Justice's (DOJ) Office of Justice Programs (OJP), which also includes the Bureau of Justice Statistics; the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention; the Office for Victims of Crime; and the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking (SMART). Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of DOJ or DHS.

Preface

This resource was developed to provide law enforcement and fusion centers with promising practices and recommendations on how to develop or enhance the process of querying Computer-Aided Dispatch (CAD) data to derive or develop information, tips and leads, or suspicious activity (including suspicious activity reports meeting the requirements outlined in the Nationwide Suspicious Activity Reporting [SAR] Initiative [NSI]). The recommendations explain how to utilize the tools and resources necessary to build this capability and offer examples of how centers and agencies may work together to exchange such information. The recommendations result from research, meetings with law enforcement and criminal intelligence experts, and site visits with several agencies and fusion centers. It is understood that agencies and fusion centers vary in their structure, size, and organizational authority and that not all guidance in this resource may be directly applied. However, the framework discussed in this resource can be adapted, scaled, and applied to a variety of organizational models.

Acknowledgements

This resource was developed with the support of the U.S. Department of Homeland Security (DHS). The information contained in this resource does not represent the views, opinions, official positions, or policies of any sole contributor, department, or agency. Rather, it was created through a dynamic and collaborative effort of multiple state, local, and federal law enforcement and criminal justice partners, practitioners, and subject-matter experts. Special thanks go to the law enforcement agencies that provided valuable contributions in the development and vetting of this resource.

I. Introduction

Law enforcement agencies and fusion centers rely on the ever-increasing levels of technology to support their operations including CAD systems. CAD serves as the control point for incoming calls for service, response histories, and other initial response functionality. CAD data has the potential to be combined with other agency data and agency analysis efforts to provide a more robust results set. This allows finite investigative resources to be better focused on those suspicious activities reasonably indicative of preoperational planning associated with terrorism or other criminal activity.

While CAD systems vary based on jurisdiction and vendor, all CAD systems serve the same function: providing a coordinated system in which dispatchers can assign and track law enforcement resources to specific calls for service. CAD systems are critical because they are often the very first point of storage and transmittal of key information collected during law enforcement interactions with members of the public.[1]

Like CAD systems, SAR workflow processes vary across the nation. These processes differ largely because of the size and responsibility of the agencies enacting them, but they mostly fit the same general functional standard model of intake, review, vet, store, and share.

II. Purpose of This Resource

The purpose of this resource is to enable agencies and fusion centers to establish a CAD query and integration process to enhance their SAR programs and subsequent analysis. This resource will enable agencies and centers to incorporate CAD data into the review and analysis of SARs; develop search queries to identify potential indicators of emerging threats (validated against prior events), such as targeted violence, by aggregating and reviewing CAD information with other available information to identify patterns; and share threat reports derived from review and analysis.

The systems and models described in this document are intended to be generic in nature and do not favor one approach over another. The promising practices discussed in this resource serve as a starting point for establishing a CAD process and building a functional suspicious activity query process.

III. Why Query Information From CAD?

Law enforcement and other public safety agencies, such as fire and emergency medical services, use CAD systems to facilitate incident response and communication in the field. CAD systems, in many cases, are the first point of entry for information coming into a law enforcement, fire, or EMS system. CAD is inclusive of many systems and requires layers of interoperability. The typical

[1] DHS Science and Technology Directorate is supporting a CAD-to-CAD Interoperability Project regarding development of a Functional Standard for CAD Systems that will standardize data elements across different systems, and ultimately support interoperability of sharing the data across multiple systems.

functions of a CAD system include resource management, call taking, location verification, dispatching, unit status management, and call disposition. CAD systems can also support responder safety through knowledge of prior calls for service (domestic violence, firearms, etc.), critical mapping capabilities, mobile data, and other critical system interfaces.

CAD systems allow public safety operations and communications to be augmented, assisted, or partially controlled by an automated system. They can include, among other capabilities, computer-controlled emergency vehicle dispatching, vehicle status, incident reporting, and management information. All aspects of a CAD system must be optimized for rapid response time and system reliability. Since time is of the essence, the CAD system must accurately provide a data and time stamp for every activity. CAD systems collect the initial information for an incident and then provide the information to one or more records management systems (RMSs). The CAD system also supports other activities that assist in the effective use of public safety resources, including shift-change roll call, "be on the lookout" (BOLO) files, and the ability to schedule a call in the future.

Some CAD systems provide the ability to flag a CAD call as a potential suspicious activity and submit that call as a SAR to the agency's intelligence/counterterrorism unit or designated fusion center.

The process of querying CAD data to identify tips, leads, and suspicious activity reasonably indicative of preoperational planning associated with terrorism or other criminal activity can enhance the analytic capabilities of fusion centers and law enforcement agencies by helping them to uncover patterns in large data sets or identify unique events that might otherwise be overlooked. Querying data is a method for identifying patterns and emerging threats. Leveraging CAD data as part of suspicious activity analysis can also help fusion centers, law enforcement, and other public safety partners better identify and share information to support a behavioral threat-assessment process. Some agencies are moving toward real-time crime centers/smart-city processes leveraging the value of real-time information that Public Safety Answering Points and CAD systems can provide.

IV. What Information Can Be Included in or Developed From CAD Data?

Tips and Leads (Including SARs)

Unique, or patterns of, information, tips, and leads, including SARs can be derived from a CAD system using a query process. Tips and leads are generally uncorroborated reports or information generated from inside or outside a law enforcement agency that allege or indicate some form of possible criminal activity.[2] They are sometimes referred to as suspicious incident reports, SARs, and/or field interview report information.

[2] Fusion Center Privacy, Civil Rights, and Civil Liberties (P/CRCL) Policy Development Template (Version 3.0) 44 (March 2019) available at https://bja.ojp.gov/library/publications/fusion-center-privacy-civil-rights-and-civil-liberties-policy-development; P/CRCL Policy Development Guide for State, Local, and Tribal Justice Entities (April

A tip or lead can come from a variety of sources, including, but not limited to, the public, field interview reports, and anonymous or confidential sources. This information may be based on mere suspicion or on a level of suspicion that is less than a "reasonable suspicion" and, without further information or analysis, it is unknown whether the information is accurate or useful. Raw data in the CAD system may have been entered as a tip, but the subsequent evaluation of the CAD data transforms the tip into a focal point by adding analytic context relevant to the threat environment and ongoing investigations.

SAR information is a subcategory of tip or lead data. A SAR is defined as "official documentation of observed behavior reasonably indicative of preoperational planning associated with terrorism or other criminal activity."[3] The SAR process focuses on gathering information about behaviors and incidents associated with crime. This process is vital to detecting, deterring, and preventing criminal activity, including terrorism. It offers a standardized means for identifying, documenting, analyzing, and sharing SARs and applying data analytic tools to the information. This makes SAR information useful for identifying trends and revealing patterns and leads. Implementation of the SAR process can be accomplished within the agency's existing framework for gathering, documenting, processing, analyzing, and reporting behaviors and incidents that are reasonably indicative of preoperational planning associated with terrorism or other criminal activity.

Investigative Information/Intelligence

The information generated through the CAD database query process and the SAR process may lead to the development of an active case investigation or criminal intelligence for further analysis. A SAR submission may lead to the investigation of a crime and will be stored in accordance with agency procedures in the agency's RMS. Investigators and analysts may also analyze the data derived from these processes to identify emerging crime trends/patterns or develop criminal intelligence (e.g., situational awareness bulletins, and intelligence reports for line officers to assist in their public safety responsibilities). If the information is analyzed and determined to meet the reasonable suspicion standard in

2012), available at https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/privacy_policy_cover_and_body_compliant.pdf .

Tips and leads information should be maintained in a secure system, similar to data that rises to the level of reasonable suspicion. Id.

[3] See Fusion Center P/CRCL Policy Development Template, Appendix A, Terms and Definitions, 43, definition of Suspicious Activity Reporting, citing the Information Sharing Environment (ISE) SAR Functional Standard, Version 1.5.5, definition of a SAR, https://bja.ojp.gov/library/publications/fusion-center-privacy-civil-rights-and-civil-liberties-policy-development or the ISE SAR Functional Standard, Version, 1.5.5, para. 5(t), https://www.dhs.gov/sites/default/files/publications/15_0223_NSI_ISE-Functional-Standard-SAR.pdf?msclkid=b8962547a6e411ec8b0c0134f2ab4499..

28 CFR Part 23, a criminal intelligence information record may be entered in or submitted to an intelligence system, subject to 28 CFR Part 23.[4]

V. Core Privacy, Civil Rights, and Civil Liberties Protections

Identifying and properly implementing privacy, civil rights, and civil liberties (P/CRCL) protections are critical to the enduring success of a CAD query process. As a fundamental step, and as a requirement to continue to receive federal funding, a fusion center seeking to establish a CAD query process must adopt and implement a P/CRCL policy at least as strong as the ISE Guidelines.[5] Furthermore, law enforcement agencies seeking to establish a CAD query process are encouraged to adopt and implement a strong P/CRCL policy.[6] The P/CRCL policy should address how the fusion center or agency handles the personally identifiable information (PII) it seeks, receives, or uses in the normal course of business.[7] Law enforcement agencies should put in place procedures to ensure that personnel have a defined objective and a valid law enforcement purpose that is supported by documentation that justifies the gathering, maintaining, or sharing of PII.

It is also important to prohibit the collection or retention of information about individuals or organizations solely on the basis of their religious, political, or social views or activities or

Privacy Impact Assessment

A privacy impact assessment (PIA) or analysis should be conducted, and protections should be developed for PII and other personal, sensitive information to ensure that such information is properly collected, maintained, or distributed. Fusion Center P/CRCL Policy Development Template, Version 3.0.

A PIA is a process by which an entity can examine the P/CRCL risks in the entity's information system and sharing activities. In general, a PIA evaluates the process through which PII is collected, stored, protected, shared, managed, and purged. By completing a PIA, entities can identify P/CRCL vulnerabilities and address and mitigate them through the design and implementation of policies. For more information, refer to PIA guidance and resources available at https://bja.ojp.gov/program/it/privacy.

The Homeland Security Information Network hosts a Community of Interest for Fusion Center Civil Liberties and Privacy Officers. This is also a valuable resource. Request access here: https://www.dhs.gov/how-join-hsin.

[4] The record must be evaluated to determine that it (i) is relevant to the identification of, and the criminal activity engaged by an individual who or organization that is reasonably suspected of involvement in criminal activity, and (ii) meets criminal intelligence system submission criteria. 28 Code of Federal Regulations Part 23, §23.3(b)(3).

[5] See Fusion Center P/CRCL Policy Development Template.

[6] See Privacy, Civil Rights, and Civil Liberties Policy Development Template for State, Local, and Tribal Justice Entities, April 2012, https://bja.ojp.gov/library/publications/privacy-civil-rights-and-civil-liberties-policy-development-template-state.

[7] A CAD query program may be developed and implemented on an interagency or interjurisdictional basis. Multiple law enforcement agencies operating disparate CAD systems may participate in a single CAD query program. Under these circumstances, the participating agencies should enter into a memorandum of agreement that defines their roles and responsibilities related to the sharing of data, information, and intelligence.

their participation in a particular noncriminal organization or lawful event.[8] And when documenting SARs, apparent or actual race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity of the individual or group must not be considered as factors creating suspicion. However, those attributes may be documented in specific suspect descriptions for identification purposes or when directly related to participation in an identified criminal activity or enterprise.[9] To give effect to key P/CRCL protections, senior executives should: (1) ensure that personnel receive appropriate guidance and training that explains how the P/CRCL protections and limitations apply to the performance of their official duties; and (2) consult with their respective legal counsel and civil liberties and privacy officers (CLPOs) to make sure that strong P/CRCL protections (including oversight and accountability mechanisms) are in place to ensure compliance with applicable laws, regulations, standards, and policies.[10]

VI. Promising Practices

The process of querying CAD data for information that supports enhanced identification of suspicious activity is currently under way by several intelligence units across the country, each finding the results of its efforts beneficial to the intelligence process. Site visits and interviews were conducted at three law enforcement agencies and fusion centers, with two primary approaches identified as promising and potentially providing replicable methods for querying CAD data. What follows is a high-level overview of these two approaches, including their general process and recommendations.

Model 1: CAD As a Stand-Alone Data Source

General Process

In this model, the agency develops a keyword search relative to suspicious activities that leverages the information found within the agency CAD system. Keyword searches are customized and refined by analysts working with agency-specific IT professionals. Categories include narrative, name search, location,[11] field interviews, business sector queries, and more. Geospatial analysis and custom search capabilities help to show patterns across jurisdictional borders.

---

[8] See Fusion Center P/CRCL Policy Development Template, E.2.

[9] Id. See also ISE-SAR FS Version 1.5.5, citing Guidance for Federal Law Enforcement Agencies regarding the Use of Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation, or Gender Identity (December 2014), https://www.dhs.gov/publication/guidance-federal-law-enforcement-agencies-regarding-use-race-ethnicity-gender-national)

[10] Agencies and centers are encouraged to have technology-related P/CRCL policies (e.g., policies governing the use of automated license plate readers, real-time and open-source analysis, face recognition). See Appendix B Resources for a list of technology-related P/CRCL policy templates that were developed under the auspices of the Criminal Intelligence Coordinating Council (CICC), Global Justice Information Sharing Initiative, and supported by the Bureau of Justice Assistance (BJA), Office of Justice Programs (OJP), and the U.S. Department of Justice (DOJ), in collaboration with DHS.

[11] This may include location data showing proximity to CIKR.

In this instance, the fusion center duplicates its CAD data and places it into a data warehouse.[12] That is, the fusion center queries mirror copies of live data. Data is moved into an independent data warehouse that restructures the data to make it searchable by analysts. This process is completed without disrupting any existing databases from the jurisdictions involved. A duplicate system is not necessary to run the suspicious activity queries on CAD data, but information technology (IT) protocols would need to be considered when querying the original or live data set.

The information in the data warehouse is automatically pulled at a standard interval.[13] This model integrates data that does not already reside in investigative, intelligence, or criminal history files or is not otherwise accessible to entities responsible for analyzing and sharing SARs.

Structured Query Language (SQL) statements are used to perform tasks such as updating or retrieving data on a database. The system automatically initiates predetermined daily queries against the text contained in the narrative of each call for a service record.

An analyst can also initiate a query, which automatically performs multiple types of queries simultaneously and returns results within minutes. This analyst-initiated process performs multiple simultaneous queries, across all sectors, while also filtering CAD data against the agency's established list of keyword search terms.

Reports can be automated daily and sent out to analysts in an email, but reports can also be run on demand. In one instance, for example, a single query can produce a 90- to 100-page document containing the results of any keyword found within each critical infrastructure sector query, as well as results of the global vocabulary search. Each keyword is highlighted to aid in review of the results. Analysts review the results daily to determine whether any of the discovered terms warrant follow-up or are false positives (e.g., *lazer* versus *laser*, *van* versus *white van*). The analysts then develop a summary report that is distributed to detectives, who examine the information in the summaries, perform follow-up, and submit relevant tips and leads to the SAR database.

A team of analysts collates information that came in from CAD, field reports, bookings, and tips and leads from the public or other agencies from the previous 24 hours. Analysts pull reports/records that are reasonably indicative of preoperational planning associated with terrorism or other criminal activity. Reports that reflect a possible threat of targeted violence are also pulled for vetting. The reports/records are brought for follow-up to a team of supervisors, which then reviews the reports and determines whether the report is reasonably indicative of preoperational planning associated with terrorism or other

[12] The methodology of accessing the CAD data could vary depending on ownership, chain-of-command, funding/contract restrictions, or other factors (e.g., a CAD system operated by the patrol division and query system operated by the criminal division). The technical methodology presented is based on a reviewed field example and is not intended to be prescriptive or limit other potential technical solutions.

[13] For high-volume events of CAD data, the automated pulls from CAD data may be set at shorter intervals (e.g., every 30 minutes).

criminal activity, whether a follow-up investigation by a detective is necessary, and whether to enter the information into the Federal Bureau of Investigation's (FBI) eGuardian system immediately (in accordance with applicable standards, policies, and procedures) or wait for further vetting.

This model can be incorporated into the suspicious activity review process and operationalized by:

1. Establishing critical infrastructure and key resources (CIKR) and tips and leads processes to handle information sources that focus on suspicious activities reasonably indicative of preoperational planning associated with terrorism or other criminal activity.

2. Adding CAD data as part of the available information resources. In this example, duplicating CAD data and storing the duplicate data in a data warehouse that auto-refreshes when the original CAD system updates.[14]

3. Developing a standard query process, determined by agency IT protocols, of the CAD data from surrounding jurisdictions.

4. Developing a list of query keywords, in coordination with legal counsel and/or CLPOs, based on a valid law enforcement purpose, maintaining/updating that list to provide the supporting justification.

5. Training analysts on technical matters so that they can initiate queries and develop reports for dissemination to agencies and centers.

6. Entering terrorism-related SARs into eGuardian in accordance with applicable standards, policies, and procedures.

7. Ensuring that subject-matter, expertise-specific training for personnel involved in this process (e.g., analysts, investigators, supervisors) is obtained on a routine basis so that the analysis of this data is conducted under the appropriate context with the ever-evolving threat environment and in compliance with applicable laws, regulations, standards, and policies.[15]

---

[14] Model 1 may be modified to include automated pulls of information from an agency's records management system (RMS) or, in the event of regional information sharing, from the RMS systems of agencies in surrounding jurisdictions. An RMS is an agencywide system that provides for the storage, retrieval, retention, manipulation, archiving, and viewing of information, records, documents, or files pertaining to law enforcement operations. This system covers the entire life span of records development—from the initial generation to its completion. IJIS Institute, Standard Functional Specifications for Law Enforcement Records Management Systems, Version III. https://cdn.ymaws.com/www.ijis.org/resource/collection/93F7DF36-8973-4B78-A190-0E786D87F74F/Standard_Functional_Specifications_for_Law_Enforcement_Records_Management_Systmes_Version_III.pdf.

[15] This should also drive the use of keywords in the queries of the system.

8. Ensuring that access to or dissemination of any products containing PII is based on a need-to-know and right-to-know (or more restrictive) basis.

9. Ensuring that sound policy, procedures, and training are developed and implemented to guide this operation while protecting the privacy, civil rights, and civil liberties of individuals (see Section V).

Model 2: CAD As an Integrated Data Source

In contrast to the first model, this model allows highly vetted and trained analysts to query data without having to duplicate and store the data in a separate warehouse. The general process differs slightly from Model 1, although the overarching outcomes remain the same.

General Process

All data is retained in a proprietary and compartmentalized database housed on a secure server. This database is accessible only by individuals within the agency's intelligence unit who have been granted special access to its compartment. Raw data, narratives, descriptions, locations, social media, and phone data are all retained in accordance with agency information retention requirements. Once entered, this information becomes searchable in a variety of ways to ensure that it has the potential to be useful in future intelligence investigations.

There are two major back-end systems set up for query in this model. One system (referenced above) contains tips and leads, proprietary intelligence reports, narrative structures, and an overview of connections among persons of interest and their criminal behavior. The other system is a CAD-like system and acts as a central platform that aggregates data from 9-1-1 calls and other internal and external sources. This system includes an interactive dashboard interface that displays real-time alerts. Analysts can then query the data as needed. This system also contains a unique pattern-recognition software developed by intelligence experts that identifies patterns among related burglaries, robberies, and grand larcenies by looking for similarities among complaint reports and scoring them to compare across data.[16]

Tips and leads that are reasonably indicative of criminal activity, including those with a potential nexus to terrorism or targeted violence, are processed through an agency with an intelligence capability or a fusion center. This process includes notification to the appropriate state, local, tribal, and territorial (SLTT) agency with jurisdiction over the activity and entry into the FBI's eGuardian system in accordance with applicable standards, policies, and procedures. Within the agency or fusion center, leads are then assigned to a unit specifically designated to follow up on tips and leads.

[16] Technical methodology presented is based on a reviewed field example and is not intended to be prescriptive or limit other potential technical solutions.

In this model, the context, facts, and circumstances of each SAR are addressed, focusing on incidents, individuals, groups, or locations. SARs that are reasonably indicative of criminal activity, including those with a potential nexus to terrorism or targeted violence, are immediately documented, vetted, and processed, as appropriate. The vetting process begins at intake, where a detective gathers as much information as possible. When appropriate, the information is sent to be analyzed by an intelligence analysis unit, a cyber component (focused specifically on open-source intelligence (OSINT) and review for online presence), a regional intelligence center, and the watch commander. Based on the merits of the information, it is then either processed and investigated by the Leads Investigation Unit, forwarded to an appropriate investigative unit (Threat Assessment Unit, etc.), or documented and retained as information that can be referenced in relation to future investigations.

This model can be incorporated into the suspicious activity review process and operationalized by:

1. Establishing a CIKR and tips and leads process to handle information sources that focus on suspicious activities reasonably indicative of preoperational planning associated with terrorism or other criminal activity.

2. Establishing a secure, compartmentalized database housed on a secure server.

3. Potentially working with a vendor(s) to build an interactive data aggregator platform and to address, during contract negotiations, any proprietary issues related to the ownership of or access to the data, in the event the agency or center terminates its contract with the vendor.

4. Processing tips and leads that are reasonably indicative of criminal activity, including those with a potential nexus to terrorism or targeted violence, through that intelligence unit by:
   a. Sending information to be analyzed by an intelligence analysis unit, a cyber component, a regional intelligence center, and a watch commander.
   b. Processing/investigating the tips and leads, forwarding the information to the appropriate investigative unit, *or* documenting and retaining as information for reference in future investigations.

5. Notifying the responsible SLTT law enforcement agency with jurisdiction over the reported activity.

6. Entering terrorism-related SARs into eGuardian in accordance with applicable standards, policies, and procedures.

7. Ensuring that subject-matter, expertise-specific training for personnel involved in this process (e.g., analysts, investigators, supervisors) is obtained on a routine basis so that

the analysis of this data is conducted under the appropriate context with the ever-evolving threat environment and in compliance with applicable laws, regulations, standards, and policies.

8. Ensuring that access to or dissemination of any products containing PII is based on a need-to-know and right-to-know basis.

9. Assigning the lead to a unit that is specifically designated to follow up on any tips or leads that require further/extensive investigation.

10. Ensuring that sound policy, procedures, and training are developed and implemented to guide this operation while protecting the privacy, civil rights, and civil liberties of individuals (see Section V).

VII. Opportunities and Challenges

Cross-Jurisdictional Data Sharing

Encouraging a culture of sharing information between agencies and across jurisdictions remains one of the biggest obstacles for agencies seeking to improve their intelligence capabilities. The nation's leading intelligence analysts and law enforcement personnel stress the critical importance of building and improving relationships with neighboring jurisdictions and private sector entities as the key to successful information sharing.[17]

A fundamental challenge faced by many jurisdictions is the lack of a centralized way to access multiple data sources. Many information systems were established over multiple years with varying business needs and business rules and could also be operated by distinct segments within an organization or even different organizations. This issue is reflective of fusion centers that are responsible for supporting a region or area of responsibility that includes multiple law enforcement agencies operating disparate CAD systems, RMS systems, etc. School systems may also have their own CAD data, but most agencies will not have access or ability to view the data.

In the first model, some neighboring agencies do not capture CAD data from other jurisdictions. However, partner agencies can run queries against their own CAD systems and use the application. Ideally, partner agencies may be provided seats in the intelligence unit or fusion center and can perform queries every few days. If an entity is considering adopting this model, the recommendation is to regularly hold regional CompStat meetings to share the resulting query information with other jurisdictions.

[17] Call to Action—A Global Unified Message Regarding Information Sharing: https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/information%20sharing%20call%20to%20action%20May%202019.pdf.

Staffing Needs

A challenge with either of these models is that replicating these processes will be difficult for agencies that, for example, have limited intelligence/analytical staff members. A data scientist or data architect could be beneficial to support this process. The recommendation is to have an IT person assigned to each agency or section for responding to IT-related requests. It is important to engage management, field officers, investigators, analysts, and IT staff during the development, implementation, and operational processes to ensure that the requirements of each level are addressed.

Vendor Selection and Data Ownership

While not inclusive of every technical challenge, several key points were identified during the site visits. Agencies indicated some level of difficulty with importing legacy data into a new system. Recommendations for navigating this area included the following:

1. Data conversion can be a significant challenge, especially if data ownership is not clearly defined within vendor contracts. Vendors may claim proprietary access issues or note significant development efforts if information sharing beyond the initial application was never a consideration when purchased.

2. By being clear up front about what is to be done with the back-end data, the intelligence unit and/or fusion center can maintain more control over its ability to query and analyze the department's data. Querying the data is different from copying the data from a database or data warehouse. If a vendor requires data access through its own proprietary interface, there may be issues with accessing that data later, especially if/when agency upgrades are made. There may also be limitations in the types of queries and the breadth of analysis that can be conducted.

3. Any potential vendor should be able to provide users with a diagram or schematics of the infrastructure of the back-end data. This can bring up intellectual property issues with vendors, but it is helpful for end users to know the "final resting place" and other important characteristics of the data for accessibility and knowledge transfer.

4. To ease the pressure of time and resource allocation on an agency or center, software updates and patches should be included in the vendor contract.

Ongoing Needs

Law enforcement agencies and fusion centers that implement this process need to be experienced in the manual query process in case of system failure or other technical difficulty. The recommendation is for analysts to complete manual queries monthly to keep their knowledge of that process fresh.

Systems interoperability is identified as an area for continued improvement and innovation. This is particularly critical as it relates to the cross-jurisdictional sharing of intelligence information.

The CAD query process will continue to develop as new agencies implement the process and current agencies refine their process. In addition, the application of new technologies, including artificial intelligence, will continue to enhance the overall process outcomes.

It is also important to understand that CIKR assets could be in a state of flux because some sectors or subsectors are transient in nature. Some types of facilities close or change locations on a routine basis, making it challenging for law enforcement to maintain accurate location data. For these reasons, maintaining and updating the geographic information system (GIS) of CIKR assets is essential. The asset inventory of CIKR must accurately reflect the geographic location of each asset and be updated accordingly. The data from the CIKR asset inventories should be integrated into the CAD query processes.

Finally, all models recommend updating the keyword search list frequently according to any current threats. Removing outdated or unnecessary terms is important to maintaining the usability of the system. It is also recommended that agencies and centers maintain business rule-development processes on file, including coordination with legal counsel and/or CLPOs, so that if questioned, they can provide documentation to support the valid law enforcement purpose for choosing a particular term or grouping of terms.

Appendix A: Glossary of Terms

Analysis (law enforcement)—The review of information and its comparison to other information to determine the meaning of the data in reference to a criminal investigation or assessment. (Fusion Center P/CRCL Policy Development Template, 35)

Computer-Aided Dispatch—CAD systems allow public safety operations and communications to be augmented, assisted, or partially controlled by an automated system. It can include, among other capabilities, computer-controlled emergency vehicle dispatching, vehicle status, incident reporting, and management information. CAD systems collect the initial information for an incident and then may provide the information to one or more RMS systems. The CAD system also supports other activities that assist in the effective use of public safety resources, including shift-change roll call, "be on the lookout" (BOLO) files, and the ability to schedule a call in the future. (Law Enforcement Information Technology Standards Council Standard Functional Specifications for Law Enforcement Computer Aided Dispatch [CAD] systems guide)

Criminal Intelligence—Information compiled, analyzed, and/or disseminated to anticipate, prevent, or monitor criminal activity. (National Criminal Intelligence Sharing Plan Version 2.0, 45 [2013], https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/e050919201-intelguide_web.pdf)

Criminal Intelligence Information—Data which has been evaluated to determine that it (i) is relevant to the identification of and the criminal activity engaged in by an individual who or organization which is reasonably suspected of involvement in criminal activity, and (ii) meets criminal intelligence system submission criteria. (28 Code of Federal Regulations Part 23, §23.3[b][3])

Intelligence Analyst—A professional position in which the incumbent is responsible for organizing various facts, documentation of circumstances, evidence, interviews, and any other material related to a crime into a logical and related framework for the purposes of developing a criminal case, explaining a criminal phenomenon, describing crime and crime trends and/or preparing materials for court and prosecution, or arriving at an assessment of a crime problem or crime group. (National Criminal Intelligence Sharing Plan Version 2.0, 46 [2013], https://bja.ojp.gov/library/publications/national-criminal-intelligence-sharing-plan-building-national-capability)

Intelligence Bulletins—A finished intelligence product in article format that describes new developments and evolving trends. The bulletins are typically sensitive but unclassified (SBU) and available for distribution to local, state, tribal, and federal law enforcement. Minimum Criminal Intelligence Training Standards, Version 2.0, Global, DOJ, October 2007, https://bja.ojp.gov/library/publications/minimum-criminal-intelligence-training-standards-law-enforcement-and-other.

Intelligence Products—Reports or documents that contain assessments, forecasts, associations, links, and other outputs from the analytic process that may be disseminated for use by law

enforcement agencies for prevention of crimes, target hardening, apprehension of offenders, and prosecution. Minimum Criminal Intelligence Training Standards, Version 2.0, Global, DOJ, October 2007, https://bja.ojp.gov/library/publications/minimum-criminal-intelligence-training-standards-law-enforcement-and-other.

Intelligence Unit—For the purposes of this resource, the term "intelligence unit" refers to any law enforcement unit designated, trained, and authorized to handle and develop criminal intelligence, including fusion centers.

Need to Know—As a result of jurisdictional, organizational, or operational necessities, access to sensitive information or intelligence is necessary for the conduct of an individual's official duties as part of an organization that has a right to know the information to perform or assist in a law enforcement, homeland security, or counterterrorism activity or other lawful and authorized government activity, such as to further an investigation or meet another law enforcement requirement. (Fusion Center P/CRCL Policy Development Template, 40)

Personally Identifiable Information (PII)—"Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual." (Fusion Center PCRCL Policy Development Template, 41)

Right to Know—A requirement for access to specific information to perform or assist in a lawful and authorized governmental function. Right to know is determined by the mission and functions of a law enforcement, homeland security, counterterrorism, or other lawful and authorized government activity or the roles and responsibilities of personnel in the course of their official duties. (Fusion Center P/CRCL Policy Development Template, 42)

Records Management System—RMS is an agencywide system that provides for the storage, retrieval, retention, manipulation, archiving, and viewing of information, records, documents, or files pertaining to law enforcement operations. RMS covers the entire life span of records development—from the initial generation to its completion. (Standard Functional Specifications for Law Enforcement Records Management Systems, Version III, IJIS Institute. https://cdn.ymaws.com/www.ijis.org/resource/collection/93F7DF36-8973-4B78-A190-0E786D87F74F/Standard_Functional_Specifications_for_Law_Enforcement_Records_Management_Systmes_Version_III.pdf)

Targeted Violence—An unlawful act of violence dangerous to human life or potentially destructive of critical infrastructure or key resources, in which actors or groups intentionally target a discernible population of individuals or venue in a manner that poses a threat to homeland security, based on (1) an apparent terrorist motive indicated by the population or venue targeted, or by the particular means of violence employed; (2) the significance of actual or potential impacts to the nation's economic security, public health, or public safety, or to the minimal operations of the economy and government; or (3) the severity and magnitude of the violence or harm and impact of either upon the capabilities of state and local governments to effectively respond without federal assistance.

Suspicious Activity Report (SAR)—Defined in the ISE-SAR Functional Standard, Version 1.5.5 as "[o]fficial documentation of observed behavior reasonably indicative of preoperational planning associated with terrorism or other criminal activity." SAR information offers a standardized means for feeding information repositories or data analysis tools. Patterns identified during SAR information analysis may be investigated in coordination with the reporting agency and, if applicable, a state or regional fusion center. SAR information is not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor is it designed to support interagency calls for service.

Tips and Leads Information or Data—Generally uncorroborated reports or information generated from inside or outside a law enforcement agency that allege or indicate some form of possible criminal activity. Tips and leads are sometimes referred to as suspicious incident report (SIR), suspicious activity report (SAR), and/or field interview report (FIR) information. However, SAR information should be viewed, at most, as a subcategory of tip or lead data.

A tip or lead can come from a variety of sources, including, but not limited to, the public, field interview reports, and anonymous or confidential sources. This information may be based on mere suspicion or on a level of suspicion that is less than "reasonable suspicion" and, without further information or analysis, it is unknown whether the information is accurate or useful. Tips and leads information falls between being of little or no use to law enforcement and being extremely valuable depending on the availability of time and resources to determine its meaning. (Fusion Center PCRCL Policy Development Template, 44)

Appendix B: Resources

ISE-SAR Functional Standard, Ver. 1.5.5, https://www.dhs.gov/sites/default/files/publications/15_0223_NSI_ISE-Functional-Standard-SAR.pdf?msclkid=b8962547a6e411ec8b0c0134f2ab4499.

28 CFR Part 23 Resources, https://28cfr.ncirc.gov/Resources.

28 CFR Part 23 Online Training, https://28cfr.ncirc.gov/.

Department of Homeland Security Strategic Framework for Countering Terrorism and Targeted Violence (September 2019), https://www.dhs.gov/publication/dhs-strategic-framework-countering-terrorism-and-targeted-violence.

National Criminal Intelligence Sharing Plan, Version 2.0, 46 (2013), https://bja.ojp.gov/library/publications/national-criminal-intelligence-sharing-plan-building-national-capability.

Minimum Criminal Intelligence Training Standards, Version 2.0, Global, DOJ, October 2007, https://bja.ojp.gov/library/publications/minimum-criminal-intelligence-training-standards-law-enforcement-and-other.

A Call to Action—A Global Unified Message Regarding Information Sharing: https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/information%20sharing%20call%20to%20action%20May%202019.pdf.

Standard Functional Specifications for Law Enforcement Records Management Systems—Version III, IJIS Institute, https://cdn.ymaws.com/www.ijis.org/resource/collection/93F7DF36-8973-4B78-A190-0E786D87F74F/Standard_Functional_Specifications_for_Law_Enforcement_Records_Management_Systmes_Version_III.pdf.

Privacy, Civil Rights, and Civil Liberties Resources

Guidance for Federal Law Enforcement Agencies Regarding the Use of Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation, or Gender Identity (December 2014), https://www.dhs.gov/publication/guidance-federal-law-enforcement-agencies-regarding-use-race-ethnicity-gender-national.

Fusion Center Privacy, Civil Rights, and Civil Liberties (P/CRCL) Policy Development Template, Version 3.0, available at https://bja.ojp.gov/library/publications/fusion-center-privacy-civil-rights-and-civil-liberties-policy-development.

P/CRCL Policy Development Guide for State, Local, and Tribal Justice Entities (April 2012), https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/privacy_policy_cover_and_body_compliant.pdf.

FBI Privacy Impact Assessment for the eGuardian System, https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/eguardian-threat.

Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations (February 2013), https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/developing_a_policy_on_the_use_of_social_media_in_intelligence_and_investigative_activities_compliant.pdf.

License Plate Reader Policy Development Template for Use in Intelligence and Investigative Activities (February 2017) https://bja.ojp.gov/library/publications/license-plate-reader-policy-development-template-use-intelligence-and.

Real-Time Open Source Analysis (ROSA) Resource Guide (July 2017), https://bja.ojp.gov/library/publications/real-time-and-open-source-analysis-rosa-resource-guide.

Recommendations for First Amendment-Protected Events for State and Local Law Enforcement Agencies (December 2011), https://bja.ojp.gov/library/publications/recommendations-first-amendment-protected-events-state-and-local-law.

Justice Information Sharing Website, U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance (informative Web page addressing Issues, Resources, and Training Justice Entities and Public Safety Agencies), https://bja.ojp.gov/program/it/privacy.