PRIORITY
Criminal Justice
NEEDS INITIATIVE

A project of the RAND Corporation,
the Police Executive Research Forum,
RTI International, and the University of Denver

Improving Information-Sharing Across Law Enforcement: Why Can't We Know?

John S. Hollywood, Zev Winkelman

Key findings

- There has been improvement on information-sharing standards among RMSs and CAD and other key systems, as well as the infrastructure for developing and using standards.
- Progress also has been made on developing repositories of shared law enforcement information at the federal, state, and regional levels and on developing common policies.
- There are strategies to improve systems' affordability, including comparatively inexpensive off-the-shelf systems, shared licensing, and software-as-a-service/cloud migration models.
- Law enforcement information-sharing architecture remains complex, and only a fraction of the interfaces are covered by standards—and those standards often overlap and conflict with each other.
- Information assurance is a special issue; while federal policies exist, it is difficult to provide adequate security.
- Some commercial providers see developing expensive custom interfaces as a key revenue source and thus do not support standardization; others are unsupportive because of the reported cost and expertise of implementing standards. That said, others see information sharing as a competitive advantage.
- A common concern focuses on how much RMSs and CAD systems cost, especially for smaller agencies.
- Commercial providers have reported challenges in gathering requirements.

SUMMARY Law enforcement agencies increasingly demand sophisticated information technology (IT) capabilities to support their operations. These capabilities depend on records management systems (RMSs), which maintain agencies' case histories, and computer-aided dispatch (CAD) systems, which maintain agencies' calls for service and call response histories. There are also increasing demands to share information with regional, state, and federal repositories of criminal justice information. While substantial progress has been made in improving the information-sharing ability and affordability of key law enforcement systems, many barriers remain. This report reviews progress to date, the sizable barriers remaining, and approaches to overcoming those barriers.

Substantial progress has been made on developing information-sharing standards among RMSs and CAD and other key systems, as well as the infrastructure for developing and using standards—notably, the National Information Exchange Model (NIEM), Global Reference Architecture (GRA), and IJIS Institute's Springboard compliance testing initiative. Progress also has been made on developing repositories of shared law enforcement information at the federal, state, and regional levels and on developing common policies and request-for-proposal (RFP) language. Finally, there are strategies to improve systems' affordability, including comparatively inexpensive off-the-shelf systems, shared licensing schemes in which agencies in a region share systems, and software-as-a-service/cloud migration models in which a third party hosts and maintains the software and hardware but the agency still controls and owns the data.

For the longer term, we recommend developing a common business process that brings together practitioners and developers in identifying requirements for law enforcement IT systems.

However, significant barriers remain. Law enforcement information-sharing architecture is complex; even at a high level, there are more than 50 desired interfaces involving RMSs and CAD systems. Only a fraction of these interfaces are covered by standards, the standards often overlap and conflict with each other, and the infrastructure for developing and testing standards is incomplete (there are no true software development kits or "read this first" instructional materials, for example). Many model policies are under development now; existing model policies and RFP language is limited. Information assurance is a special issue; while federal policies exist, it is still difficult to provide adequate security. For example, this may involve having to change typical default software configurations and constantly check users' compliance.

Incentives and business models for commercial providers can be problematic. There are providers who see developing expensive custom interfaces as a key revenue source and thus do not support standardization; there are also providers who are unsupportive because of the reported cost and expertise of implementing standards. One encouraging sign is that there are commercial providers who see standards and information-sharing mechanisms as a key competitive advantage. Commercial providers have also reported challenges in gathering requirements from clients, including inaccuracy, excessive customization, and broad specifications to "share everything."

Regarding affordability, it is common to hear concerns about how much RMSs and CAD systems cost, especially for smaller agencies. Cost concerns are especially high because of budget cutbacks in recent years.

To address these barriers in the short term, we have identified items to include in RFPs related to: complying with NIEM and GRA; connecting to specific federal, state, and regional systems; ease of exporting data from RMSs and CAD systems; and checking information-sharing capabilities during the acquisition process. We identify indicators that can help agencies determine whether bidding providers are interested in supporting information-sharing at comparatively low costs. We discuss writing requirements that inform bidders about what agencies would like to accomplish, finding companies that target the agency's size, conducting testing and evaluation during the bidding process, and pursuing new business models (e.g., software-as-a-service or regionalization).

For the longer term, we recommend developing a common business process that brings together practitioners and developers in identifying requirements for law enforcement IT systems. We also recommend creating a multilayer framework for sharing law enforcement information, extending on earlier efforts. This framework should include a master data model describing how to share data elements used across multiple standards, software development kits for building and implementing standards, and expanded testing and certification. It should also include critical interfaces that have not yet been captured in existing or planned standards. We present elements to be included in future policy and RFP language related to information-sharing, information-assurance, and privacy and civil rights. Finally we recommend further support for the new technology and business models that can help make these systems more affordable, helping to move from "why can't we know?" to "we do know."

WHY CAN'T WE KNOW?

"The ability to share knowledge across the department is key. What is going on at a very local level, what is working, who is where? Just the ability to share knowledge . . . Nobody really knows what is in every box or in every system right now, you don't know what is in production or in staging."

"We need to be interoperable. What do you want to get back? How is it captured? How can it be seen, in what format? Come up with those standards . . . we need universal interoperability."

— From interviews to assess law enforcement's most pressing information technology needs (Gordon et al., 2012)[1]

Law enforcement agencies increasingly demand sophisticated IT capabilities to support their operations, from determining identification (ID) and prior histories of persons stopped in the field, to supporting detectives in their investigations, to providing strategic information to commanders. These capabilities depend heavily on sharing information. Core IT systems include RMSs, which maintain agencies' case histories, and CAD systems, which maintain agencies' calls for service and call-response histories. Beyond these systems are increasing demands to access and share information with regional, state, and federal repositories of criminal justice information. However, given the number of systems involved, as well as the complexity of criminal justice information, information-sharing today is a difficult and expensive proposition.

The National Institute of Justice (NIJ) has studied the problems of sharing information over the years, with a great deal of work on interoperable voice communications. One well-known guide is *Why Can't We Talk?* (National Task Force on Interoperability, 2005). In recent discussions, practitioners have reported progress in being able to communicate by voice across agency boundaries during major events. Admittedly, one approach is having the largest agency in a metropolitan region maintain crates of radios to distribute during major events, but solutions and workarounds like this do exist.

However, practitioners have reported far spottier progress when it comes to sharing data. Difficulties are compounded by affordability issues in RMSs, CAD systems, and information-sharing technologies, especially given widespread budget cuts.[2] The question appears to be moving from "why can't we talk?" to "why can't we know?" This report considers both barriers to and progress on information-sharing to date and presents possible ways ahead for both near-term acquisition and long-term technology and policy development.

METHODOLOGY

This report consolidates reports on information-sharing needs, barriers, progress, and opportunities that draw on a combination of expert practitioner advisory panels, interviews and focus groups with agency representatives, conferences, prior reports on information-sharing, and information-sharing standards reference material. Key discussions with practitioners and technical experts included:

- interviews and focus groups with agencies and developers, most notably during RAND's *Keeping Law Enforcement Connected* study (Gordon et al., 2012).
- panels and presentations from various conferences, including the International Association of Chiefs of Police (IACP) conferences (2011–2015), International Association of Crime Analysts (IACA) conferences (2012–2014), IJIS Institute winter briefings (2012–2014), Global Justice Information Sharing Initiative meetings (2012–2013), and 2012 and 2015 Workshops on Information Sharing and Safeguarding, which are sponsored by the IJIS Institute and Object Management Group (OMG), in coordination with the Program Manager, Information Sharing Environment (PM-ISE).
- input, especially on policy and technology needs, from NIJ advisory panels, including the 2011 Technology Working Groups, 2013 Law Enforcement Advisory Panel, 2014 Law Enforcement Futures Panel, and 2014 Future Web Technologies Panel. These panels and needs are discussed fully in the RAND report *High-Priority Information Technology Needs for Law Enforcement* (Hollywood et al., 2015).

Key materials reviewed include:

- *Priority Data Exchanges for Local Communications Centers: A List of Data Exchanges Relating to Computer Aided Dispatch Systems* from the IJIS Institute and Association of Public Communications Officials (APCO)–International (Parker and Wisely, 2009), *High Priority Information Sharing Needs for Emergency Communications and First Responders* (Unified CAD Project Committee, 2012), and *Recommendations of the Emergency Communications Task Force* from the IJIS Institute and APCO–International (Wisely, Wormeli, and Gabbin, 2013).[3]
- *Standard Functional Specifications for Law Enforcement Records Management System* from Law Enforcement Information Technology Standards Council (LEITSC) (2010).

- *Why Can't We Share?* from the National Criminal Justice Association (NCJA) Initiative (NCJA, 2004).
- The Global Justice Information Sharing Initiative's information-sharing standards packages (Global Standards Council, undated).
- Standards packages uploaded to the Office of Justice Programs' (OJP's) Information Exchange Packet Documentation (IEPD) Clearinghouse (OJP, undated-b). (IEPD refers to a key type of information-sharing standard described later.)

The next section discusses information-sharing needs commonly reported by practitioners in the material cited above. We begin with a brief history of IT systems and corresponding needs, then consider contemporary needs for information, and finally discuss the technology and policy elements necessary to enable information-sharing. We then consider progress to date on improving sharing and review outstanding barriers. Finally, we discuss near-term recommendations for agencies procuring core IT systems, as well as longer-term technology and policy recommendations to help transition from "why can't we know?" to "we do know."

NEEDS FOR LAW ENFORCEMENT INFORMATION-SHARING

A Brief History of IT for Law Enforcement

Law enforcement IT systems have undergone at least two major iterations and are in the midst of a third. In the mainframe era of computing, monolithic COBOL-based installations replaced processes that were largely manual and paper-based.[4] Some of these early mainframe systems facilitated communication with field units via "dumb" mobile data terminals that could receive and display messages (Micro Focus, 2011).

The commodity hardware and PC revolution led to the next stage in law enforcement IT. As hardware costs dropped, communities that had smaller budgets or were looking to trim larger budgets began to consider the benefits of less expensive RMSs and CAD systems (Gortcinsky and Gagne, 1992). This demand was met by developers eager to supply solutions to new customers on new platforms. Enhanced 911 has added caller ID and location data. The spread of geographic information systems (GISs) and Global Positioning System (GPS)–capable computing allowed for the addition of field unit locations, addresses, incident locations and histories, and other geospatial data. At the same time, mobile data computers emerged as an alternative to the less-capable data terminals for enhancing the capabilities of units in the field (Morgan, 2003). This iteration of law enforcement IT also marked increasing demands for interoperability, not only among multiple types of calls for service (e.g., police, fire, emergency management service [EMS]) but also among local, state, and federal systems.[5]

Several trends shape the current IT environment. The first is the continuation of Moore's law, resulting in continuing exponential growth in computing power at continually lower cost. This phenomenon extends beyond processing speed, memory size, hard disk size, or network capacity when one considers the number of sophisticated sensors that now come standard on an average commodity smartphone. As a result, however, expectations continue to rise regarding the availability of low-cost capabilities, both in the operations center and in the field.

The second is the rise of "big data," which can be briefly summarized as extremely large data sets that cannot be processed using traditional database applications on stand-alone machines. These can include 911 call records, cases, digital evidence repositories, offender registries, video from stationary and mobile cameras, automated license plate reader hits, tracking data on both law enforcement vehicles and offenders with tracking bracelets, and so on. *FedTech* magazine, for example, has claimed that "what had been a data sharing challenge has evolved into a Big Data opportunity" (Grimes, 2013). In principle, such data sets are available through centralized data warehouses and federated query systems.

The desire to share law enforcement information is not new; McEwen (2002), for example, notes that the desire to share data is, in some ways, merely an evolution of the earlier desire to use data stored in the mainframe to collect performance metrics, detect hotspots, or feed queuing models to

Law enforcement IT systems have undergone at least two major iterations and are in the midst of a third.

optimize staff levels or patrol routes. The importance of sharing is also established; Duval (2008), for example, notes that criminal networks are aware of information-sharing limitations, especially across smaller agencies, and exploit those limitations in their actions.

Broadly speaking, there are two categories of information-sharing needs. The first involves the exchange of data in defined transactions. Examples of these include calls for service, routing dispatch requests, or the submission or querying of crime incident data to federal databases. The second typically involves fusing data—such as sensor feeds, video feeds, social media data, or collections of disparate external records—to search for patterns and make predictions (Grimes, 2013).[6]

These two challenges occasionally pull standards in opposing directions. On the one hand, greater universal standardization of data exchanges that are transactional in nature would increase capabilities to share information across a wide number of stakeholders who might be asymmetrically resourced otherwise. On the other hand, stakeholders pushing the bounds on what can be done with data fusion constantly will be racing ahead of defining rigorous standards for data exchange in the absence of coordination.

Types and Sources of Information Needed

Figures 1, 2, and 3 show the major types of information that we observed being commonly called for throughout the materials and meetings described above. The figures show which law enforcement roles need the various types of information and the sources of that information. Figure 1 presents tactical policing information that is needed by officers and deputies on patrol, for making field contacts, and for conducting service calls. Figure 2 presents information needed by agency personnel carrying out both crime analyses and crime investigation activities. Figure 3 presents policing information needs at the operational (command and operations center) level, including needs for operations management, agency capabilities development, incident command, and communicating with the public. While a number of source systems are named, some of the most common include:

- the agency's local RMS and CAD system
- RMSs and CAD systems in neighboring jurisdictions
- state, regional, and federal repositories of criminal justice and criminal justice–relevant information (examples for the latter include weather services and pawned-item databases).

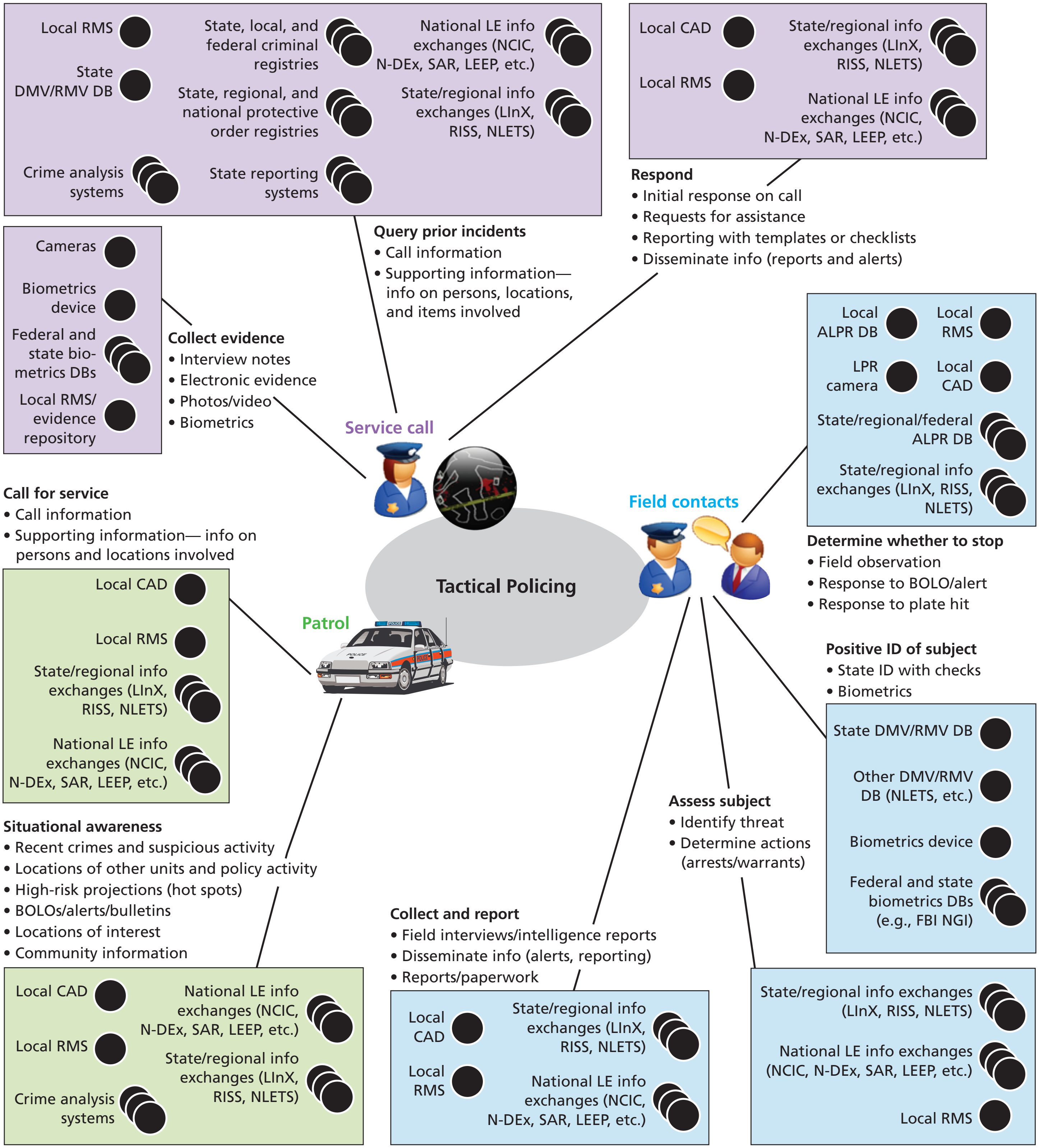
Figure 4 considers system-to-system connection needs. Single nodes reflect information-sharing for a single system; multiple nodes reflect sharing among a family of related systems (e.g., multiple criminal registries at the local, state, and federal levels). Connections previously assessed as critical to be supported via interoperability standards are shown in bold. The network is a dual hub-and-spoke layout with the local agency's RMS and CAD system as the two hubs.

Criticality assessments came from *Priority Data Exchanges* (Parker and Wisely, 2009, pp. 70–72, "Top 12 Links"), *High Priority Information Sharing Needs* and *Recommendations of the Emergency Communications Task Force* (Unified CAD Project Committee, 2012, pp. 6–7, "Critical Information Exchanges"), and *Why Can't We Share?* (NCJA, 2004). Links previously identified as "critical" tend to be high-volume data connections in which the two systems commonly come from different providers or across agency and other organizations at the local, state, and federal levels.

This figure is greatly simplified, as key regional, state, and some federal systems are treated generically or consolidated into a single link. Some examples of federal, regional, and state repositories that an RMS/CAD system might need to connect with include:

- *National Data Exchange (N-DEx).* This system is a cloud-hosted data warehouse that serves as a law enforcement search engine. It contains more than 180 million records and tracks more than 1 billion entities (people, places, and events). In addition to returning search query results, N-DEx uses proprietary algorithms to help law enforcement "connect the dots" between what may otherwise seem like unrelated data. In addition to documentation on the Federal Bureau of Investigation's (FBI's) N-DEx website (FBI, undated, the IJIS Institute provides an introductory guide to connecting to N-DEx (Chawdry et al., 2013).
- *National Law Enforcement Telecommunications System (NLETS).* NLETS is a state-owned nonprofit organization that facilitates more than 100 interstate data exchange transactions. Examples include drivers' license photos and registry of motor vehicles information, Interpol records, state criminal records, and corrections photos (NLETS, 2015).
- The *San Diego Association of Governments' Automated Regional Justice Information System* (ARJIS) provides a number of information services to dozens of local, state, and federal agencies in the San Diego region (ARJIS, undated). Examples include providing data from multiple

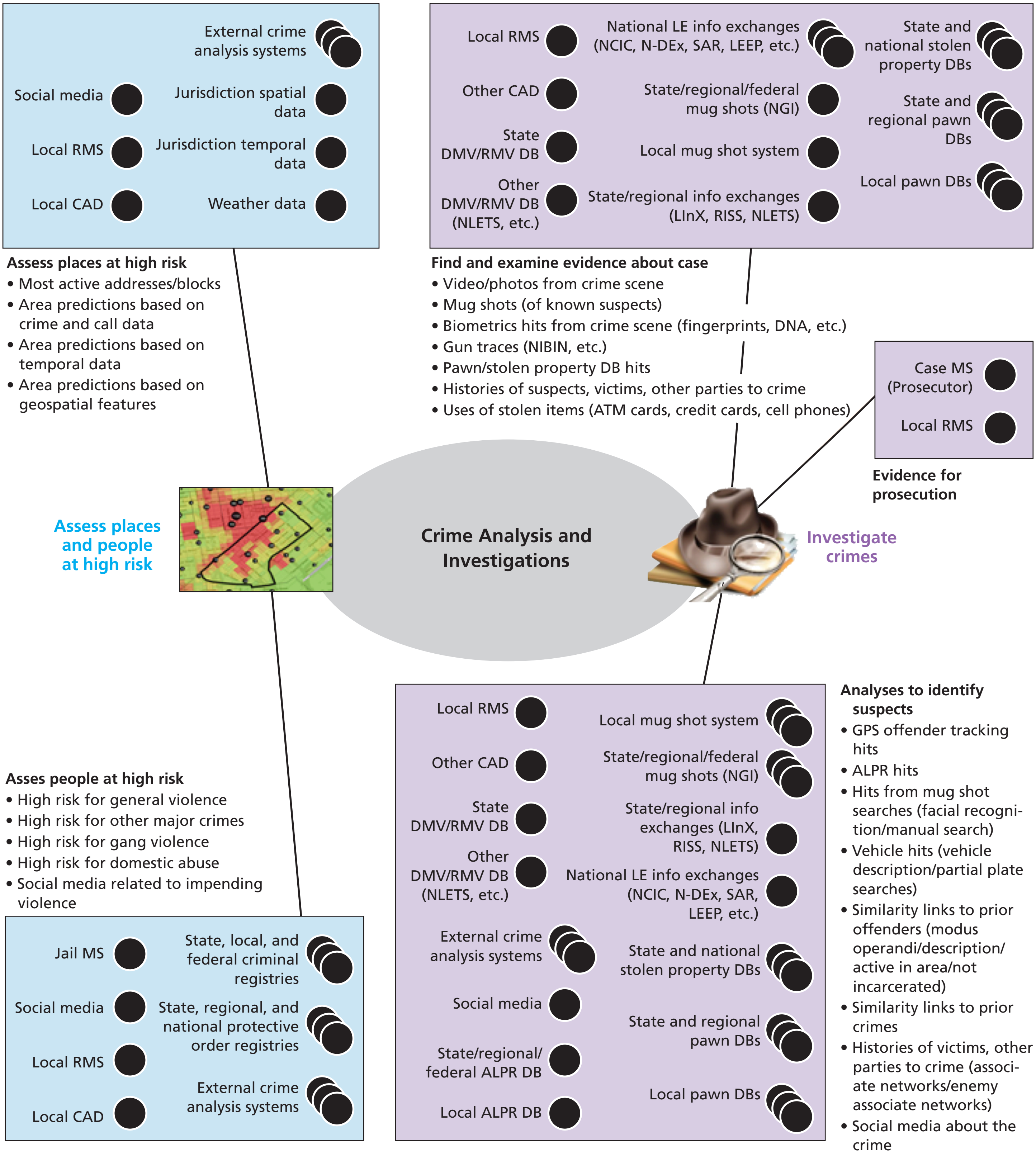
Figure 1. Information Needs for Tactical Policing


Local RMS
State DMV/RMV DB
Crime analysis systems
State, local, and federal criminal registries
State, regional, and national protective order registries
State reporting systems
National LE info exchanges (NCIC, N-DEx, SAR, LEEP, etc.)
State/regional info exchanges (LInX, RISS, NLETS)
Local CAD
Local RMS
State/regional info exchanges (LInX, RISS, NLETS)
National LE info exchanges (NCIC, N-DEx, SAR, LEEP, etc.)
Respond
• Initial response on call
• Requests for assistance
• Reporting with templates or checklists
• Disseminate info (reports and alerts)
Query prior incidents
• Call information
• Supporting information— info on persons, locations, and items involved
Cameras
Biometrics device
Federal and state bio-metrics DBs
Local RMS/ evidence repository
Collect evidence
• Interview notes
• Electronic evidence
• Photos/video
• Biometrics
Service call
Local ALPR DB
Local RMS
LPR camera
Local CAD
State/regional/federal ALPR DB
State/regional info exchanges (LInX, RISS, NLETS)
Field contacts
Determine whether to stop
• Field observation
• Response to BOLO/alert
• Response to plate hit
Call for service
• Call information
• Supporting information— info on persons and locations involved
Tactical Policing
Local CAD
Local RMS
State/regional info exchanges (LInX, RISS, NLETS)
National LE info exchanges (NCIC, N-DEx, SAR, LEEP, etc.)
Patrol
Positive ID of subject
• State ID with checks
• Biometrics
State DMV/RMV DB
Other DMV/RMV DB (NLETS, etc.)
Biometrics device
Federal and state biometrics DBs (e.g., FBI NGI)
Assess subject
• Identify threat
• Determine actions (arrests/warrants)
Situational awareness
• Recent crimes and suspicious activity
• Locations of other units and policy activity
• High-risk projections (hot spots)
• BOLOs/alerts/bulletins
• Locations of interest
• Community information
Collect and report
• Field interviews/intelligence reports
• Disseminate info (alerts, reporting)
• Reports/paperwork
Local CAD
Local RMS
Crime analysis systems
National LE info exchanges (NCIC, N-DEx, SAR, LEEP, etc.)
State/regional info exchanges (LInX, RISS, NLETS)
Local CAD
Local RMS
State/regional info exchanges (LInX, RISS, NLETS)
National LE info exchanges (NCIC, N-DEx, SAR, LEEP, etc.)
State/regional info exchanges (LInX, RISS, NLETS)
National LE info exchanges (NCIC, N-DEx, SAR, LEEP, etc.)
Local RMS

NOTE: ALPR=automated license plate recognition; BOLO="be on the lookout;" DBs=databases; DMV=Department of Motor Vehicles; LE=law enforcement; LEEP= Law Enforcement Enterprise Portal; LInX=Law Enforcement Information Exchange; NCIC=National Crime Information Center; RMV=Registry of Motor Vehicles; SAR=Suspicious Activity Report.

RAND *RR645-1*

Figure 2. Information Needs for Crime Analyses and Criminal Investigations


External crime analysis systems
Social media
Jurisdiction spatial data
Local RMS
Jurisdiction temporal data
Local CAD
Weather data

Assess places at high risk
- Most active addresses/blocks
- Area predictions based on crime and call data
- Area predictions based on temporal data
- Area predictions based on geospatial features

Local RMS
National LE info exchanges (NCIC, N-DEx, SAR, LEEP, etc.)
State and national stolen property DBs
Other CAD
State/regional/federal mug shots (NGI)
State and regional pawn DBs
State DMV/RMV DB
Local mug shot system
Local pawn DBs
Other DMV/RMV DB (NLETS, etc.)
State/regional info exchanges (LInX, RISS, NLETS)

Find and examine evidence about case
- Video/photos from crime scene
- Mug shots (of known suspects)
- Biometrics hits from crime scene (fingerprints, DNA, etc.)
- Gun traces (NIBIN, etc.)
- Pawn/stolen property DB hits
- Histories of suspects, victims, other parties to crime
- Uses of stolen items (ATM cards, credit cards, cell phones)

Evidence for prosecution

Assess places and people at high risk
Crime Analysis and Investigations
Investigate crimes

Asses people at high risk
- High risk for general violence
- High risk for other major crimes
- High risk for gang violence
- High risk for domestic abuse
- Social media related to impending violence

Jail MS
State, local, and federal criminal registries
Social media
State, regional, and national protective order registries
Local RMS
External crime analysis systems
Local CAD

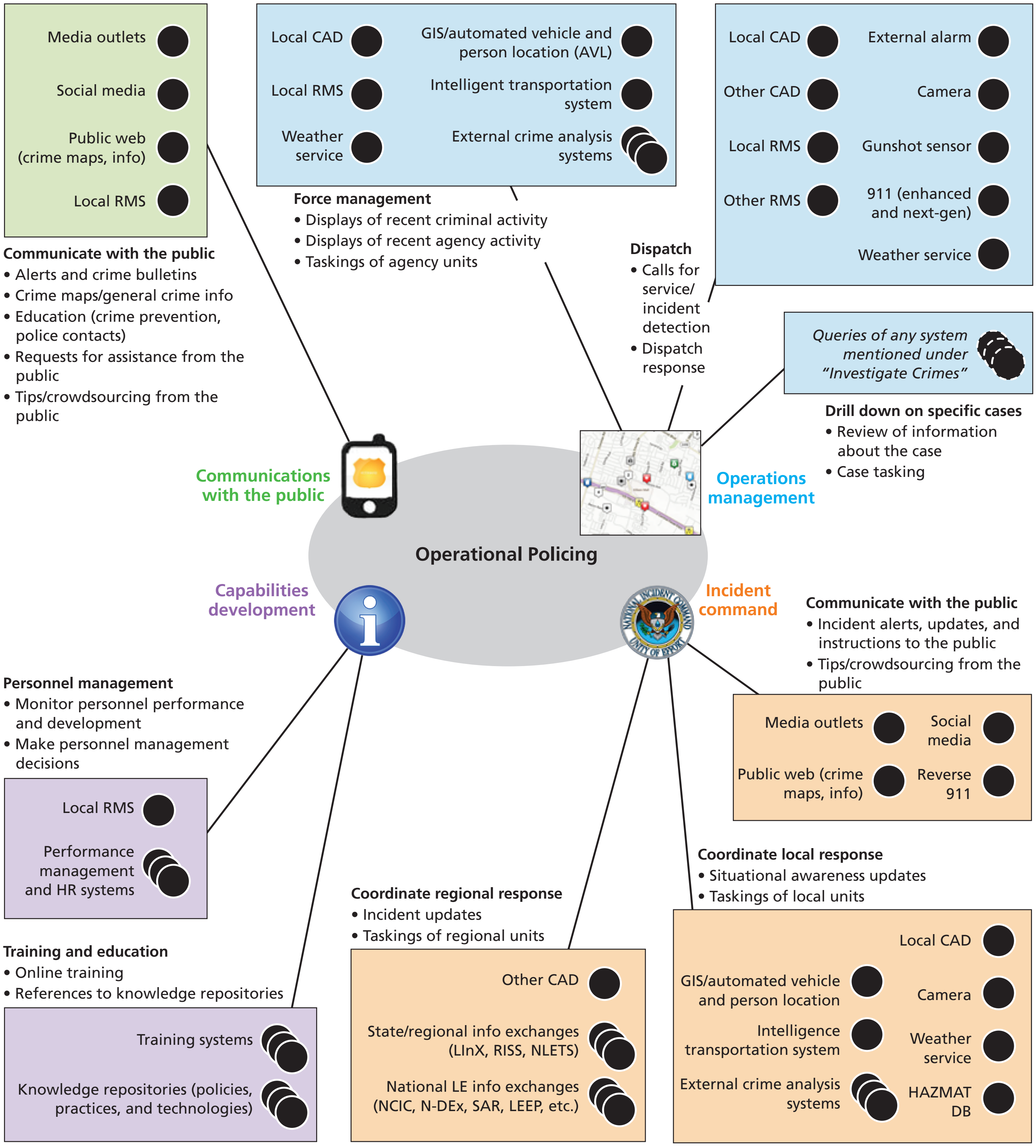
Local RMS
Local mug shot system
Other CAD
State/regional/federal mug shots (NGI)
State DMV/RMV DB
State/regional info exchanges (LInX, RISS, NLETS)
Other DMV/RMV DB (NLETS, etc.)
National LE info exchanges (NCIC, N-DEx, SAR, LEEP, etc.)
External crime analysis systems
State and national stolen property DBs
Social media
State and regional pawn DBs
State/regional/ federal ALPR DB
Local pawn DBs
Local ALPR DB

Analyses to identify suspects
- GPS offender tracking hits
- ALPR hits
- Hits from mug shot searches (facial recognition/manual search)
- Vehicle hits (vehicle description/partial plate searches)
- Similarity links to prior offenders (modus operandi/description/ active in area/not incarcerated)
- Similarity links to prior crimes
- Histories of victims, other parties to crime (associate networks/enemy associate networks)
- Social media about the crime

NOTE: MS=management system; NGI=next-generation identification; and NIBIN=National Integrated Ballistic Information Network.

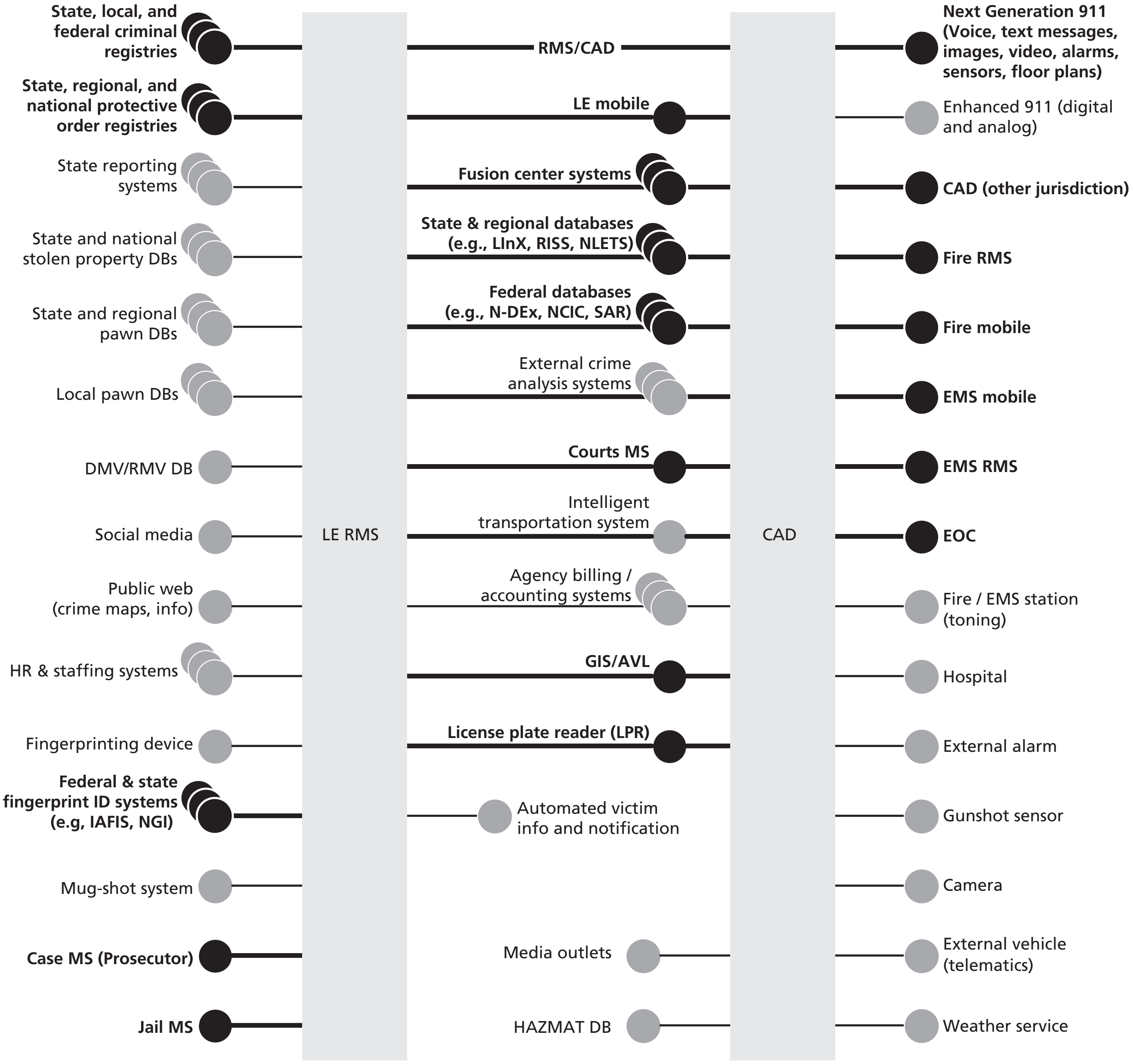
RAND *RR645-2*

Figure 3. Information Needs for Operational Policing


Media outlets ●
Social media ●
Public web (crime maps, info) ●
Local RMS ●
Communicate with the public
• Alerts and crime bulletins
• Crime maps/general crime info
• Education (crime prevention, police contacts)
• Requests for assistance from the public
• Tips/crowdsourcing from the public
Local CAD ●
Local RMS ●
Weather service ●
GIS/automated vehicle and person location (AVL) ●
Intelligent transportation system ●
External crime analysis systems ●
Force management
• Displays of recent criminal activity
• Displays of recent agency activity
• Taskings of agency units
Local CAD ●
Other CAD ●
Local RMS ●
Other RMS ●
External alarm ●
Camera ●
Gunshot sensor ●
911 (enhanced and next-gen) ●
Weather service ●
Dispatch
• Calls for service/ incident detection
• Dispatch response
Queries of any system mentioned under "Investigate Crimes" ●
Drill down on specific cases
• Review of information about the case
• Case tasking
Communications with the public
Operations management
Operational Policing
Capabilities development
Incident command
Communicate with the public
• Incident alerts, updates, and instructions to the public
• Tips/crowdsourcing from the public
Media outlets ●
Social media ●
Public web (crime maps, info) ●
Reverse 911 ●
Personnel management
• Monitor personnel performance and development
• Make personnel management decisions
Local RMS ●
Performance management and HR systems ●
Training and education
• Online training
• References to knowledge repositories
Training systems ●
Knowledge repositories (policies, practices, and technologies) ●
Coordinate regional response
• Incident updates
• Taskings of regional units
Other CAD ●
State/regional info exchanges (LInX, RISS, NLETS) ●
National LE info exchanges (NCIC, N-DEx, SAR, LEEP, etc.) ●
Coordinate local response
• Situational awareness updates
• Taskings of local units
Local CAD ●
GIS/automated vehicle and person location ●
Camera ●
Intelligence transportation system ●
Weather service ●
External crime analysis systems ●
HAZMAT DB ●

RAND *RR645-3*

Figure 4. Needs for Law Enforcement System-to-System Connections


State, local, and federal criminal registries
State, regional, and national protective order registries
State reporting systems
State and national stolen property DBs
State and regional pawn DBs
Local pawn DBs
DMV/RMV DB
Social media
Public web (crime maps, info)
HR & staffing systems
Fingerprinting device
Federal & state fingerprint ID systems (e.g, IAFIS, NGI)
Mug-shot system
Case MS (Prosecutor)
Jail MS
LE RMS
RMS/CAD
LE mobile
Fusion center systems
State & regional databases (e.g., LInX, RISS, NLETS)
Federal databases (e.g., N-DEx, NCIC, SAR)
External crime analysis systems
Courts MS
Intelligent transportation system
Agency billing / accounting systems
GIS/AVL
License plate reader (LPR)
Automated victim info and notification
Media outlets
HAZMAT DB
CAD
Next Generation 911 (Voice, text messages, images, video, alarms, sensors, floor plans)
Enhanced 911 (digital and analog)
CAD (other jurisdiction)
Fire RMS
Fire mobile
EMS mobile
EMS RMS
EOC
Fire / EMS station (toning)
Hospital
External alarm
Gunshot sensor
Camera
External vehicle (telematics)
Weather service

NOTES: Bold links assessed as critical. IAFIS=Integrated Automated Fingerprint Identification System; and EOC=Emergency Operations Center.

RAND *RR645-4*

systems in response to officers' queries about a field contact's history, as well as providing a notification service so that when one officer makes a contact with another regarding a person of interest (such as a person under community supervision), both officers receive an alert.

- The *Alaska Law Enforcement Information Sharing System* (ALEISS) supports record-sharing across incompatible RMSs. ALEISS provides a secure location for housing hardware, administrative records for cleared technical staff, routine security compliance audits, training records, and evaluation metrics on the system (National Law Enforcement and Corrections Technology Center, 2006). The online platform allows users to execute searches that consolidate results across the multiple RMSs (ALEISS, undated; Andrews, undated).
- The *Law Enforcement Information Exchange* (LInX) is a regional aggregator run by the U.S. Navy that has grown to cover ten regions and 1,350 organizations. The Navy pays for areas near its bases, but other regions such as Atlanta and South Carolina have paid to maintain access (Mitchell, 2013).
- The *Regional Information Sharing System* (RISS) is a family of systems that support criminal investigations. RISS currently includes six regional networks. Specific RISS services include databases of information on gangs, terrorism and homeland security, and officer safety and investigation deconfliction, as well as records submitted by state and local participants on past offenses and offenders (RISS, undated).

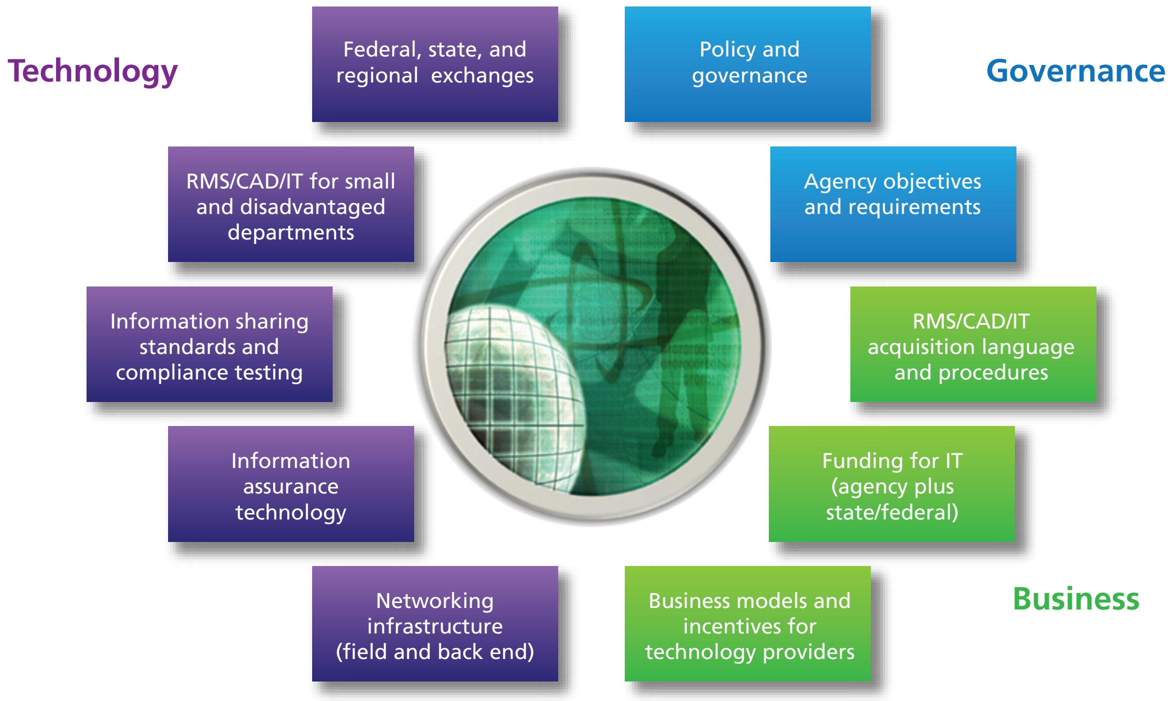
Enablers for Information-Sharing

To bring about information-sharing across the types, roles, and systems shown in Figures 1–4 requires a series of enablers that collectively form a sharing "infostructure." These enablers include not just technical tools but also governance and business models. The enablers are summarized in Figure 5.

Technology enablers are the elements most commonly thought of as supporting information-sharing and include:

- standards for sharing information, along with the architectures for employing the standards and testing mechanisms for checking compliance
- federal, state, and regional exchanges and repositories for sharing various types of information across agency boundaries
- information-assurance technology intended to ensure continued access to, and integrity and protection of, sensitive law enforcement information in the face of cyberattacks, natural disasters, and routine maintenance problems

Figure 5. Key Enablers for Information-Sharing


Technology
Federal, state, and regional exchanges
Policy and governance
Governance
RMS/CAD/IT for small and disadvantaged departments
Agency objectives and requirements
Information sharing standards and compliance testing
RMS/CAD/IT acquisition language and procedures
Information assurance technology
Funding for IT (agency plus state/federal)
Networking infrastructure (field and back end)
Business models and incentives for technology providers
Business

RAND *RR645-5*

- infrastructure for physically storing and transporting information, including networks in the field and in the backend data center. Infrastructure can also include common software tools for accessing and using law enforcement information.

Governance enablers set the strategy and direction for using technologies in ways that meet the acceptance of the public. Major elements include:

- agency objectives and requirements for RMSs and CAD and other key IT systems, identifying what the systems are supposed to do to support law enforcement operations successfully.
- governance organizations for designing and enforcing policies and procedures. Key policy areas that have risen to the forefront in recent years include information-assurance (security), civil rights, and privacy.

Finally, business model enablers provide the funding and processes needed to bring RMSs and CAD and other key IT systems from strategy to actuality:

- Funding for IT projects—local, state, or federal—is a prerequisite for IT systems acquisition and maintenance.
- Acquisition language and procedures describe how IT system procurement, installation, and maintenance will work in support of achieving system objectives.
- Business models and incentives for technology providers, if properly set, will lead to providers focusing their efforts on helping agencies achieve information-sharing with affordable systems.

BARRIERS AND OPPORTUNITIES TO INFORMATION-SHARING

Next, we discuss progress, outstanding barriers, and opportunities for information-sharing in law enforcement.

Technology Barriers and Opportunities

As we all know, all we need to do to get to interoperability is [random stream of buzzwords]. [Laughter]

—Adapted from a workshop focusing on information-sharing

[Following a presentation on the growing cyberthreat to law enforcement networks] Q. Let's assume I'm properly scared by this, but that I know nothing other than maybe to buy a commercial Internet security package. Where do I go to start learning what to do?

A. It's hard to say now, other than some groups are working on it . . .

—Adapted from a conference session on cybersecurity

Major strides have been made in the technology supporting information-sharing. That said, there is still a great deal to accomplish. While it is possible for agencies to share information using current technology, it is not easy, much less the default.

Web services, NIEM, and GRA as a baseline. Modern information-sharing systems have largely converged on the use of web services exchanging extensible markup language (XML) messages to share data. However, the use of XML and web services does not automatically generate seamless information-sharing. It is possible to know that data are being exchanged within a certain general format but not be able to interpret what is being shared. That requires detailed data-sharing standards.

To help specify the "language" for sharing criminal justice information, the U.S. Department of Justice (DoJ), through the Global Justice Information Sharing Initiative, developed the Global Justice XML Data Model (GJXDM). In 2007, GJXDM became a domain in NIEM, which is a partnership between DoJ and the Department of Homeland Security (DHS). Both are composed of core standards and IEPDs for sharing specific types of information in support of particular missions. (NIEM Program Management Office, 2015).

The GRA provides guidance and instruction on how to create the reusable services that perform information-sharing functions. The GRA prescribes that services be built using web services (which are lower-level system connections enabling data exchange). NIEM IEPDs specify measures to secure the data, such as encryption, and policies describing how organizations will share information (typically in documents such as service-level agreements) (Office of Justice Programs, undated-c).

NIEM and GRA provide important assistance to help build data-sharing standards (the IEPDs). However, these are effectively construction kits to help facilitate information-sharing mechanisms; they do not constitute sharing mechanisms themselves.

IEPDs. As of January 2014, there were 241 IEPDs in the DoJ's *IEPD Clearinghouse* (Office of Justice Programs, 2014) with 176 tagged as "law enforcement." Reflecting both a major strength and weakness, IEPDs can be prepared and submitted by any party (or parties) that seeks to share a specified set of data elements as described in the IEPD, compliant with the top-level NIEM specifications. The bulk of the IEPDs pertain to how specified agencies or regions intend to share specified data among themselves. There are several dozen IEPDs that have been intended for nationwide, wide-scale use; these are shown in Table 1.

Figure 6 reproduces Figure 4, modified with links supported by at least one NIEM IEPD intended for nationwide use in blue and links missing any IEPDs shown in red (Pointers to IEPDs: Parker and Wisely, 2009; IACP, undated-a; Global Standards Council, undated; and OJP, undated-c). The blue labeling merely indicates the *existence* of a relevant IEPD—it does not describe the maturity of the IEPD or the extent to which the IEPD has been deployed in fielded systems. The figure is an oversimplification, given that a number of the links apply to broad categories of differing regional, state, or federal

Table 1. Law Enforcement RMS/CAD IEPDs

Link(s)	IEPD(s)	Sponsor
CAD—Next-generation 911	Emergency incident data (EID) document	National Emergency Number Association (NENA)/APCO[a]
CAD—External CAD	Summary call for service information Detailed call for service information Request for resource Available resource response Resource availability query Request unit status update Unit status update	LEITSC[b] LEITSC LEITSC LEITSC LEITSC LEITSC LEITSC
CAD-RMS	CAD to RMS transfer	LEITSC
RMS-External RMS	RMS query RMS summary response	LEITSC LEITSC
RMS—Federal databases (SAR reporting)	Suspicious activity reporting (SAR)	Global Standards Council[c]
RMS—RMS/Courts MS/ Case MS/Jail MS (offender lifecycle reporting)	Person information availability Arrest warrant information (5 packages) Charging Inmate release information Supervision conditions summary Offender transfer notification Sex Offender Registration and Notification Act interjurisdictional relocation Prosecutor arrest warrant	Global Standards Council Global Standards Council Global Standards Council Global Standards Council Global Standards Council Global Standards Council Global Standards Council IJIS Institute[d]
RMS—Automated victim notification	Victim notification	Global Standards Council
RMS—Fingerprint systems	Fingerprint service	Global Standards Council
RMS—Federal databases (N-DEx reporting)	National Data Exchange (N-DEx) Incident/Arrest N-DEx Incarceration/Booking/Probation/Parole	FBI Criminal Justice Information Services (CJIS) FBI CJIS
RMS/CAD—Intelligent Transportation System (ITS)	ITS/Public Safety (12 packages)	IJIS Institute

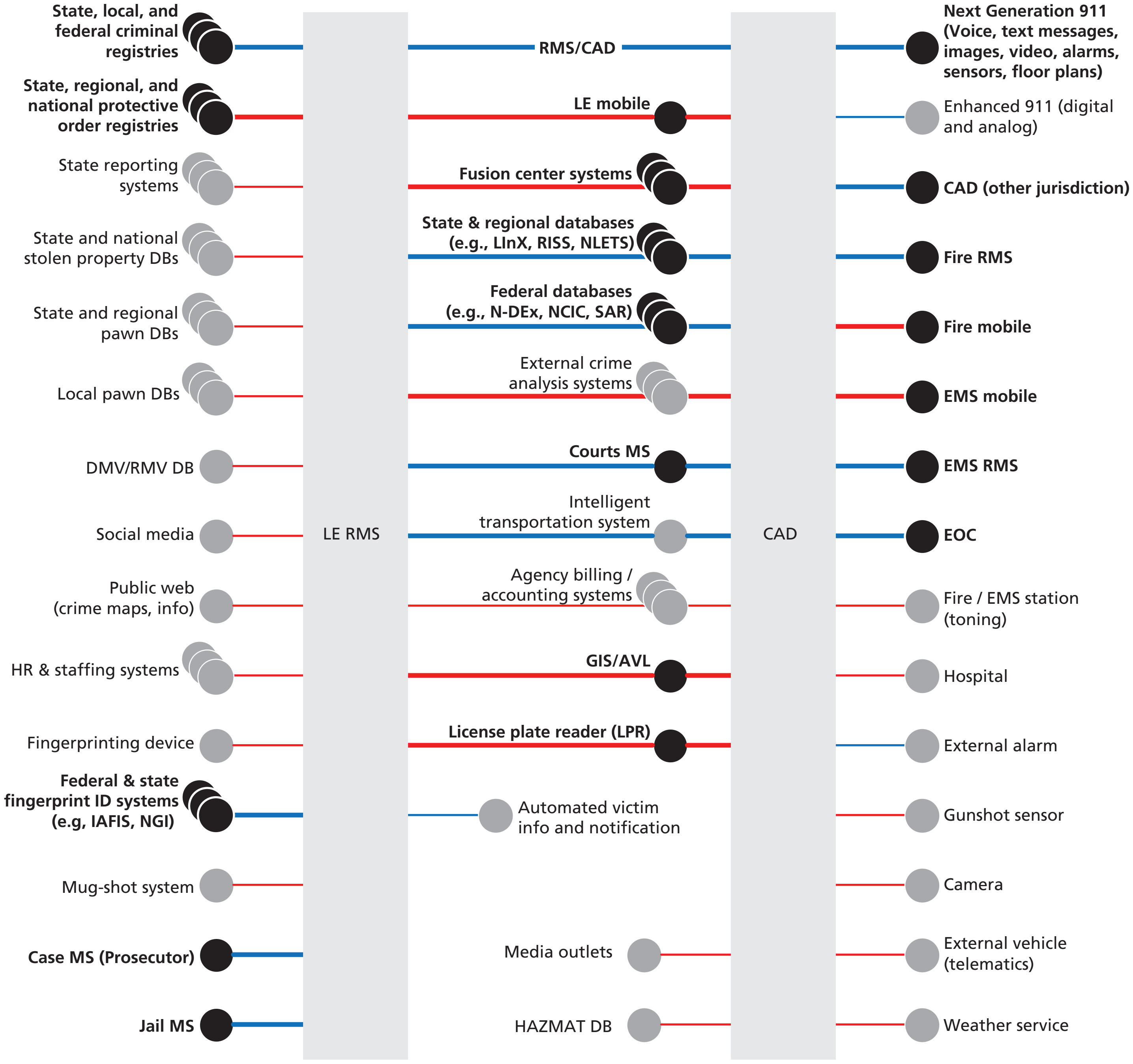
[a] As of October 15, 2013, in draft information document form only—no IEPD yet.

[b] LEITSC-sponsored IEPDs are available from the IACP's web page (2013).

[c] The Global Standards Council–sponsored packages are available from the Global Standards Council's web page on the packages (undated). Note that these packages contain implementation information in addition to NIEM-compliant IEPDs, notably on compliance with the GRA.

[d] IEPDs from others are available directly from OJP (undated-b), as are LEITSC and Global Justice Information Sharing Initiative IEPDs.

Figure 6. Top-Level Architecture Links with NIEM IEPDs


State, local, and federal criminal registries
State, regional, and national protective order registries
State reporting systems
State and national stolen property DBs
State and regional pawn DBs
Local pawn DBs
DMV/RMV DB
Social media
Public web (crime maps, info)
HR & staffing systems
Fingerprinting device
Federal & state fingerprint ID systems (e.g, IAFIS, NGI)
Mug-shot system
Case MS (Prosecutor)
Jail MS
LE RMS
RMS/CAD
LE mobile
Fusion center systems
State & regional databases (e.g., LInX, RISS, NLETS)
Federal databases (e.g., N-DEx, NCIC, SAR)
External crime analysis systems
Courts MS
Intelligent transportation system
Agency billing / accounting systems
GIS/AVL
License plate reader (LPR)
Automated victim info and notification
Media outlets
HAZMAT DB
CAD
Next Generation 911 (Voice, text messages, images, video, alarms, sensors, floor plans)
Enhanced 911 (digital and analog)
CAD (other jurisdiction)
Fire RMS
Fire mobile
EMS mobile
EMS RMS
EOC
Fire / EMS station (toning)
Hospital
External alarm
Gunshot sensor
Camera
External vehicle (telematics)
Weather service

NOTE: Bold links assessed as critical; blue=IEPDs exist; red=no IEPDs exist to date.

RAND *RR645-6*

systems. Nonetheless, even this simplified figure has 53 links and we only found IEPDs intended for nationwide use for 16. Critical links missing IEPDs include CAD systems to mobile units and CAD systems or RMSs to state and regional fusion center systems.

The number of links in the figure suggests a larger problem. It likely will be infeasible to independently develop, implement, and test so many separate data exchange standards, much less maintain consistency across them. A more integrated and efficient approach will be needed.

Emerging Technologies of Interest. Several emerging technologies are worth noting for their potential to expedite information-sharing. In brief, these include *semantic tagging*, which characterizes the content of information stored on a web document, as well as relationships with information stored elsewhere, as opposed to traditional web tagging that focuses just on how to display information (e.g., Brickley and Miller, 2014). Tags can also specify security requirements to access or modify information, making them a potential solution to certain cybersecurity difficulties. (We discuss this further below.)

Semantic tags fit in well with another emerging technology, *document-oriented databases*. Traditional databases store data in structured tables, making it difficult to add new fields or lists of new information. Document-oriented databases store information in text documents in which structured information is marked with specified tags (e.g., Lerman, 2011). This approach makes it extremely easy to update data—for example, to add a new conviction to a subject's criminal history document, along with links to related information about that conviction. It also makes it easy to query a subject's complete criminal history—the system only has to return one document, rather than piece together criminal history events across a range of data tables and systems.[7]

Training, Verification, and Validation. Requests for additional training material starting with introductory "read this first" tutorials and checklists have been made. Note that NIEM now offers detailed in-person and online training via its website.

There have been requests for NIEM and GRA to go further than they do to provide developers with true software development kits, including verification and testing tools. The IJIS Institute is now offering testing and certification of standards compliance under its Springboard program, which provides "conformance packages" on what is needed to meet the standard (including standards artifacts, samples of compliant data, and utilities to support internal testing). The program runs software/hardware-in-the-loop tests to confirm the correct exchange of standard-compliant NIEM/XML messages. Tools passing the tests are given a certification of compliance. As of July 2013, IJIS planned to support conformance testing and certification of 22 standards (IJIS, July 26, 2013).

Brittle Implementations of Standards. A related problem has to do with the implementation of XML and web services. Ideally, these are supposed to support graceful degradation, meaning that even if a system cannot understand some data elements it receives, it can still understand (and properly process) the others. Interviewees have reported brittle implementations in which systems insist on seeing an exact sequence of fields and data formats, just as with traditional structured data-sharing.

Cybersecurity. A similar "possible but not easy" issue concerns cybersecurity. There has been growing concern about increasing attacks on law enforcement systems, with such consequences as the personal information of officers and persons reporting crimes exposed (e.g., Foy, 2012) and having to pay hackers to ransom data.[8] In a recent IACP membership survey, 11 percent of respondents reported having been attacked in the preceding year, with another 20 percent unsure (Academica Group, May 22, 2013).

Progress has been made in this area. The FBI's CJIS Division maintains a core set of information assurance (IA) policies and measures that agencies and providers need to adopt to get full access to FBI CJIS systems (FBI CJIS, 2014). The IACP, RAND, and Police Executive Research Forum (PERF) with support from the Bureau of Justice Assistance (BJA), have developed a web portal to provide training and resources on cybersecurity and cybercrime issues, with the latter including resources on investigation and digital forensics techniques (IACP, undated-b). The Global Justice Information Sharing Initiative's Global Federated Identity and Privilege Management (GFIPM) toolkit supports positively identifying and authenticating users, ensuring that they have access to the information they need while controlling access to information they do not, as well as auditing usage. It also supports single-sign on, which means law enforcement personnel only have to sign with a set of credentials once to access information across a variety of systems (OJP, undated-a). As mentioned, semantic tags can specify security requirements to access or modify information. In addition, there is an emerging technology called Trustmarks that permits both users and information providers to get certified tags (the trustmarks) describing the security measures to which they comply, including the auditing mechanisms checking compliance. The technology makes it possible to automatically identify whether users and information sources across different

A fairly common way of describing standards is to relate them to electrical plugs and wires; another approach is to treat data as generic objects. Both are inaccurate.

organizations can share based on matching roles and trustmarks (Georgia Tech Research Institute, 2014).

That said, securing systems requires a good bit of time and expertise; secure status is far from the default. As an example, Grimes (2011) published a "handy checklist" for key tasks needed to secure personal computers. The list contains two dozen items, a number of which involve modifying default configurations and removing software typically installed by default.

Oversimplications of Information-Sharing Challenges. Beyond any specific technology, the ways in which information-sharing mechanisms are conceptualized can be overly simplified. A fairly common way of describing standards is to relate them to electrical plugs and wires; another approach is to treat data as generic objects. Both are inaccurate—data-sharing involves much more complexity than plugging into the electrical grid or moving generic objects around (which assume data do not have to be treated in context). The other extreme is to describe data-sharing in terms of a large amount of restricted technical jargon that even those with a computing background may not understand easily; the first quote at the beginning of this section is from a joke about this during a workshop.

Governance and Policy Barriers and Opportunities

Defining Requirements

"We all say we are completely unique and have completely unique IT needs—and we really don't, at least not more than a few."

"Stop us before we kill again."

—Adapted from workshops on information-sharing

Several documents provide agencies with references on features for major IT systems, notably RMSs and CAD systems, as well as guidance in acquiring them. LEITSC developed several documents to assist agencies with acquisition of RMSs and CAD systems, including a *CAD Functional Specification* (LEITSC, 2006), an *RMS Functional Specification* (LEITSC, 2008), and a *Project Manager's Guide to RMS/CAD System Software Acquisition* (LEITSC, 2009). The functional specifications for these systems include information-sharing; the *Project Manager's Guide* includes a general discussion of information-sharing standards, including NIEM and IEPDs. The APCO International and IJIS Institute developed an updated functional standard for CAD systems (APCO International and IJIS Institute, August 2012).

Specific guidance on information-sharing requirements, however, is limited. Notably, cross-system information-sharing discussions in the *RMS* and *CAD Functional Specifications*, as well the *Project Manager's Guide*, are fairly high-level.

We have observed two major agency-generated barriers to information-sharing related to setting requirements that result, in part, from the lack of guidance. The first is setting requirements that force developers to customize virtually all aspects of RMSs and CAD systems. This, in part, is reported to reflect a belief that each agency is unique in some respects and that all IT must be customized accordingly. However, such high degrees of customization strongly limit information-sharing (because data representations are unique) and can have very high costs.

The second barrier is not providing fully formed requirements that specify what data are to be shared and how. Instead, providers have reported having received requirements as broad as "be interoperable" or "share everything." A recent variant is "be compliant with NIEM/GRA," which, as described above, is necessary but not sufficient to share mission-specific law enforcement data. When agencies, or groups of agencies, have specified lists of data elements to share, the result has sometimes been overwhelming; the National Law Enforcement and Corrections Technology Center of Excellence on Information and Geospatial Technology (hereafter referred to as the Center) at the NIJ learned of a case in which agencies initially wanted to share more than 1,000 data fields just to describe gangs and gang members. In working with a developer, the agencies reduced the list to 37 elements.

In response, practitioners have reasonably noted that law enforcement officials are not IT experts who can readily give detailed technical requirements. There have been calls for developers to work with practitioners to understand how their operations work and their corresponding operational needs for information, then convert those operational needs to technical requirements themselves.

Governance of Standards: Too Many Solutions, Not Enough Control

"We don't have a technology problem—we have a governance problem."

"Too many groups have tried to solve the problem by making yet another standard . . . a standard intended to supersede them all just ends up being another inconsistent standard."

—Adapted from a workshop on information-sharing

"There are five ways to write zip codes . . ."

"There are seven ways to write geospatial coordinates . . ."

"There are close to 15 valid 'flavors' of Geospatial Markup Language . . ."

"There are over 200 attributes to describe a person . . . pick a new one . . ."

—Adapted from comments during Center-conducted focus groups and interviews on information-sharing

Governance issues commonly have been cited as major sources of barriers to information-sharing. Table 1's list of NIEM IEPDs include IEPDs from five different sponsors. This number does not include literally dozens of other standards-making bodies, nor all the standards created by regional and local groups; as mentioned, there were far more than 100 law enforcement–related standards in the OJP repository developed for local use. In addition to making it unclear which of many competing standards should be used, standards proliferation commonly results in inconsistency across those standards. At best, a product adapting one standard will be partly interoperable with a product adapting another standard; for example, a system using one standardized format for geospatial coordinates will not be able to share them with systems using a different format without translation.

Progress has been made in this area. The new Standards Coordinating Council (SCC) is a consortium of the PM-ISE and 14 standards development organizations created to coordinate standards prioritization and governance activities. The SCC maintains a catalog of information-sharing and safeguarding tools, resources, and case studies on its Project Interoperability website (PM-ISE, undated), as well as a list of open-access standards on its "Standards" web page (Standards Coordinating Council, 2015). However, SCC participants openly admit that, given the SCC's newness (announced January 2014), work to date has focused on standing up the SCC and identifying and listing standards and other tools, with the result that the website is currently a loosely organized collection. Coordination and integration activities are scheduled for the future.

More broadly, participants in information-sharing workshops have noted frustration that most information-sharing expansions using the standards have been piecemeal, described as pilots, experiments, limited tests, or demonstrations. There have been calls for a focus on widely deploying the standards, not just continuing to sponsor pilots and experiments with them.

Political and Policy Barriers

The states don't like the feds telling them what to do . . . There's a hesitancy. Are we really going to give everything we know about everybody to the FBI? It's a huge Big Brother.

—Quoted in Mitchell (2013)

There is often a hesitancy in agencies sharing law enforcement data. Reported reasons have to do with data owners wanting to retain strict control over "their" data, as well as concerns about what might happen to the data and how they might be used if shared outside their own systems.

A key part of the lack of trust is a lack of standardized policy documents describing exactly how data will be used and protected after sharing. To a certain extent, lack of standardized policy is similar to a technology issue—right now, too many policy documents, including point-to-point interagency sharing agreements, are largely custom-written. These include policies on strict conditions for usage, access control, other information assurance provisions, and audit procedures to

Governance issues commonly have been cited as major sources of barriers to information-sharing.

make sure those provisions are followed. These policies should help reduce data owners' concerns about sharing their data, as well as make it easier to set up the permissions for information-sharing. However, these efforts are in progress. For example, in January 2014, the IACP *Technology Clearinghouse* published a request for samples of interagency information-sharing memoranda of understanding (IACP, undated-c).

Business Model Barriers

When Information-Sharing Does Not Pay

"They're described as 'the only system you will ever need'—and they had better be, since they're not interoperable with anything else."

"There's a case in which agencies in a region decided to solve information-sharing problems once and for all by buying exactly the same version of the same RMS/CAD system. Then the vendor started working with each agency to customize their system. By the time the vendor was done, the only thing the agencies could share was 'date.'"

—Adapted from Center-sponsored focus groups on information-sharing

There is too much money to be made in writing custom interfaces to support data standardization.

—Adapted from a workshop on information-sharing

Center researchers have had discussions on three incentives for providers of RMSs and CAD systems to oppose information-sharing standardization. The first is system lock-in—some providers want to keep their client agencies dependent on their systems for as many IT activities as possible, and data standards negate lock-in potential. Some providers even resist allowing agencies to export their own data in understandable formats so the data can be used other systems. As an example, RAND provided technical assistance to an agency whose RMS and CAD system exported location coordinates as proprietary "pixels"; the vendor did not provide any method to convert these pixels into a standard data format that could be utilized in other analytic or records systems.[9]

The second is revenue from tailoring systems precisely to a client agency's specifications (custom incident type codes, etc.), which, as noted in the quote above, can lead to inabilities to share data. The third is revenue from writing custom interfaces between the RMS or CAD system and other key information systems, such as the federal systems (Naval Criminal Investigative Service [NCIS], N-DEx, etc.), state repositories, and regionally adjacent RMS or CAD systems.

Similarly, Center researchers have had discussions with commercial providers on two major disincentives for developers to support standardized information. The first is the cost and difficulty of supporting standardized information-sharing, given the architectural, technology, and governance complications described above. The second is that maintaining consistency with standards that are considered out of date is an obstacle to the developer providing innovative products and services.

Conversely, Center researchers have had a number of discussions with developers who described information-sharing as one of their key competitive advantages and revenue sources. The first emerging incentive is that offering off-the-shelf information-sharing capabilities (with, say, NCIS and N-DEx), along with methods and technologies for writing custom interfaces at low cost (for example, to share with regional repositories) is an attractive and increasingly required feature. The second is that information-sharing supports the development of innovative services. An example would be a mobile service that rapidly queries a number of federal, state, and regional systems to provide historical information on a person an officer has stopped in the field.

Budget Constraints

In this environment, agencies' top priorities are budget, budget, and budget.

—IACP President Mark A. Marshall (2011)

Due to the recession starting in 2008, as well as waves of austerity measures taken at all levels of government, law enforcement agencies have been under great budget pressures. Not surprisingly, technology, including IT purchases, has taken a hit; PERF found, in a 2010 survey of its members, 55 percent of responding departments were "cutting back or eliminating plans to acquire technology" (PERF, 2010, p. 2).

That said, the Office of Community Oriented Policing Services (October, 2011) found a number of examples of departments and associations describing technologies as force multipliers, implying that IT investments could be justified if a solid case for how they would improve effectiveness and efficiency were made. Right now, for example, it is common for agencies running noninteroperable CAD systems to have to transfer call

New models are emerging to address IT total lifecycle cost issues, notably cloud and software-as-a-service (SaaS) solutions.

and incident report information manually. Manual transfers introduce delays from re-interviewing the caller and manual data reentry, as well as data loss in cases where calls are terminated.[10] Affordability is an acute issue for small and medium-sized departments, which have far smaller budgets to begin with. As noted, NIJ and the Center are aware of comparatively inexpensive off-the-shelf RMSs and CAD systems tailored for smaller agencies, although it is unclear how aware agencies are of those offerings.

Agencies are facing other costs well beyond RMS/CAD fees. These include the cost of IT staff (employees or contractors) and the cost of building out the communications network. Network costs typically include agency-built assets (usually radio networks) and hardline and mobile Internet connections (e.g., monthly wireless subscription and data usage fees).

New Models for IT. New models are emerging to address IT total lifecycle cost issues, notably cloud and software-as-a-service (SaaS) solutions. For example, East Hampton, N.Y., recently migrated its RMSs and CAD systems to the cloud. Moving to the cloud reportedly required securing buy-in from key stakeholders, but it did transition away from capital expenses to an operating expense strategy, and focused human resources on policing rather than IT management (Tiburon Inc., 2012).

SaaS models enable multijurisdictional deployments, overhead sharing, and easy information-sharing (within the platforms). Multiple departments pay subscription fees to have a third-party provider set up and maintain RMSs, CAD systems, and other key software and data; agency users access the systems through web browsers or other "thin client" software. The hardware hosting the software and databases can be hosted on either the vendor's cloud service or locally secured servers (Crosswind Technologies, undated). South Dakota, for example, has supported providing web-based shared services, RMSs, and mobile capabilities to small agencies that previously did not have them (Milstead, 2013; New World Systems, 2010).

Note that SaaS does not require a remote cloud. In 2008, the Erlanger, Ky., Police Department started using an SaaS business intelligence platform called WebFOCUS. The system is interoperable with ten surrounding agencies, allowing information about criminal activity to accompany criminals across jurisdictions. The common aversion to sharing IT systems was overcome by the economic incentives of not having to build (and pay for) systems independently (Wyllie, 2010).

In principle, cloud and SaaS offerings could increase information-sharing by making it easier to deploy an RMS (or other system) that conforms to information exchange standards. The burden of housing data in NIEM-compliant formats would be shifted to the SaaS provider, for example (Duval, 2008). SaaS and cloud-based solutions could also make it easier for agencies of all sizes to manage the volumes of data associated from new technologies, such as mobile, fixed, and body-worn video cameras (Wyllie, 2013).

Several factors have been barriers to moving law enforcement data to the cloud. First is security, which can be a major challenge for SaaS vendors (Falkenrath, 2011).[11] As one example, the Los Angeles Police Department tried to move its email service to Google Apps for Government, but the service was unable to meet CJIS requirements (Gould, 2011). In discussions regarding cloud and SaaS models, the security of law enforcement–sensitive data is frequently discussed, including whether civilian contractors could physically manage sensitive information. That said, a common response was to ask if agency systems were really that secure now, and whether they would be more secure if professionals ran them. CJIS policy has clarified that network security rules are cloud-compatible (FBI, February 2012). However, CJIS has emphasized two challenging requirements: first, that staff with access to criminal justice information must pass fingerprint-based background checks; second, that maintenance on systems containing CJIS information cannot be performed from outside the United States (Gould, 2012).[12]

Service reliability is an additional concern. A cloud-based infrastructure can be more reliable than an on-premises system, especially during a disaster, as the systems can be replicated in places far away from the disaster.[13] However, one fear is that when power, telecom, and wireless towers are down, network connectivity will be compromised and cloud and SaaS-based solutions will fail. Locally installed backup systems with batteries are a potential response (Policesoftware, undated).

Limitations of Open Source and Government-Funded Systems

NIJ frequently receives questions about why the federal government does not fund a free, open-source RMS/CAD system. NIJ did fund CAPSIT OpenRMS, an initiative to build an open source, and therefore free, RMS system, that could be made available to smaller agencies (Porter, 2007a; Porter, 2007b). There were problems that led to the project not being successful:

- RMSs and CAD systems are not like stand-alone productivity or gaming applications—one cannot simply provide agencies with a set of installation CDs. Instead, deploying OpenRMS—or any future CAD/RMS—requires substantial cost in hardware, communications infrastructure, converting previous RMS/CAD data to the new system, systems integration, and systems administration. While the software itself could be made freely available, all of those other expenses still represent a real barrier to adoption of the system.
- Even if an initial version of a software system is paid for by the government, how to fund additional versions of the software, ongoing maintenance, and technical support remains an open question. Without ongoing funding or a license model that was "open" enough to allow a community of developers from the general public to form, the open-source use of the software fizzled out.

This case is an example of a larger problem sometimes referred to as "the valley of death"—government (or other) funding is provided to support initial development of a system, but there is no subsequent funding to maintain and improve the system, much less use it in cases where deployment has large costs (as it does for RMS/CAD).

CONCLUSIONS—TOWARD INFORMATION-SHARING

We begin with short-term recommendations for agencies facing near-term systems acquisition decisions. We make recommendations on near-term language for RFPs, finding a commercial provider interested in information-sharing, and other steps in the acquisition process. We conclude with longer-term technology development and policy recommendations; these include development of a requirements-identification business process, integration of standards development and testing, further development of model policy and RFP language, and further development and deployment of cloud and SaaS models.

Recommendations for Procuring RMS/CAD Systems

These are intended to be additions to the existing material in the *RMS Functional Specifications* (LEITSC, 2010), the *CAD Functional Specifications* (LEITSC, 2008), and the *Project Manager's Guide to RMS/CAD System Software Acquisition* (LEITSC, 2009).

Near-term language for RFPs on data-sharing standards. Purchasing agencies should recognize that existing nationwide standards, technologies, and guidance are necessary but not yet sufficient. There is not yet a definitive set of data-sharing standards with which an RMS/CAD provider should comply. That said, what does exist should be included in RFP language. In particular, we recommend that agencies:

- Request compliance with NIEM and GRA, including reading and writing NIEM/GRA-compliant messages (service requests and responses). Candidate providers should include source material and translated messages, as well as demonstrate sending and receiving NIEM-compliant messages.
- Request a description for how candidate providers use NIEM, GRA, and data-sharing standards to implement interfaces. This is important, given that providers will be called upon to incorporate a number of additional interfaces as the number of standards grows and matures.
- Request demonstrations on exporting data from the system, including samples of what the exported data look like. (Systems that permit ready data exporting make it easy for third parties to write interfaces and develop new services as needed.)
- Agencies should ask for conformance with the following current standards:
  - – CJIS information assurance policy
  - – major FBI CJIS systems,[14] including:
    - ❍ N-DEx
    - ❍ National Crime Information Center (NCIC)

- ❍ IAFIS, along with its successor, Next Generation Identification, which will include biometrics in addition to fingerprints
- ❍ Unified Crime Reports (UCR)
- ❍ National Incident-Based Reporting System (NIBRS).

– the NLETS services used by the agency's state

– the regional data-sharing portals (and underlying standards) used by the agency's state and/or region. Examples might include LInX installations, RISS installations, and data-sharing networks developed independently by states and regions

– interfaces to share data with the local prosecutor's office and jail

- confirmation of compliance with the above, such as demonstrations, test results, and references. Over time, as standards and standards testing mature, agencies will be able to request certification.

Finding a commercial provider interested in information-sharing. As noted, the Center has observed substantial variation in how commercial providers treat information-sharing. Some providers view standardized sharing as precluding revenues from lock-in or custom coding; others treat information-sharing in general as a competitive advantage. It should be noted that this distinction is not clean; a provider may be a leader in one area of the field but not want to be involved in another. Given the growing importance of information-sharing, we recommend that agencies consider providers that lean toward supporting the practice. Here are some example indicators of whether a provider is supportive:

- Ready compliance with the RFP language described above. Difficulties or high costs in supporting the standards for core federal and regional systems (NCIC, N-DEx, IAFIS, NLETS services, LInX, etc.) should be of concern. Difficulties and high costs in being able to export the agencies' own data—or exporting the data strictly in proprietary formats that are difficult if not impossible to translate—should be of special concern.
- Agencies can ask for price estimates to add interfaces as the operational need arises. Providers treating information-sharing as a competitive advantage will typically have technologies and processes to develop interfaces quickly and inexpensively. A company charging several hundred thousand dollars to provide a single interface should be a concern, unless there are major complications justifying the cost (very large scale, extreme novelty, extreme complexity, etc.). A related question is what happens if NIEM-compliant data fields are imported out of order. If the answer is the entire data import fails (e.g., the provider's implementation of XML data–sharing mechanisms is brittle, as discussed previously), that should be of concern.
- While follow-up is needed, there is some value in examining companies' presentations and promotional materials to see if they emphasize their capabilities to share information. It also might be useful to see what the companies have done previously in supporting data-sharing standards.

Additional notes on acquisition strategies. In writing RFPs, agencies should specify use cases for how they want to share information (among whom, when, under what conditions, and for what operational purpose). These do not have to be technical descriptions—in fact, they should not be, unless the agency has technical personnel who can write them— a few paragraphs with supporting diagrams describing the agencies' vision for information-sharing are sufficient.

It is also useful to identify what must be strictly implemented and what is flexible. Too much inflexibility will come at a high price and result in inabilities to share information with other agencies; at the same time, agencies should rightly expect some degree of tailoring to meet their needs. As mentioned above, RFPs can help agencies get a sense of what is readily doable.

During the selection process, we suggest that agencies follow lessons learned from the Palm Beach County Sheriff's Office's RMS/CAD acquisition (Ott and Gorrell, 2013):

- Ensure the RFP has specific terms that match what the agency wants to do. To get a better sense of what capabilities are available, seek demonstrations from multiple vendors.

In writing RFPs, agencies should specify use cases for how they want to share information.

- During the bidding process, have the bidders conduct onsite demonstrations that include tests of how well the systems can process real agency data in key scenarios (not just canned demo data).
- Gaps between the vendor's system and the agency's desired system that need to be fixed in the final installation should be expressed explicitly in the final contract.
- Determine milestones (including payment milestones) for delivered capability, along with criteria testing whether that capability has actually been delivered.
- Identify and track resolution of installation and implementation problems.
- Plan for extensive configuration, testing, and training before the system goes online. Testing should specifically include interfaces; practitioners have often reported new systems being harder to use than old ones.

We also recommend that agencies consider searching for a provider who specializes in systems for that agency's size. Companies specializing in high-end, large-scale complex systems and implementation processes will result in high cost and possibly inadequate attention for smaller departments, but such complexity will be needed for successful implementations for large cities and regions. Conversely, companies specializing in smaller-scale RMSs and CAD systems will provide much more responsiveness at less cost, but may have difficulties dealing with large installations. Small agencies may want to consider cloud-based and/or regionally shared service offerings, as these appear to be promising approaches to provide smaller agencies with key capabilities at comparatively low cost and effort. That said, in pursuing cloud and regionally shared offerings, agencies need to check on information assurance procedures, starting with CJIS policy compliance. We suspect that enthusiasm for cloud offerings may change (and policies will tighten) after the first big data breach of law enforcement data in the cloud occurs. We reiterate that permitting some degree of flexibility in implementation details can greatly lower costs.

Technology Development and Policy Recommendations

We describe technology and policy steps that would help address the barriers to information-sharing, building on the progress that has been made to date.

Technology Recommendations

Integration of data standard development processes. As noted, existing standards for sharing criminal justice information (notably IEPDs) are partial and inconsistent, and NIEM and the GRA are necessary but not sufficient to achieve integration. In recognition of this issue, the IJIS/APCO *Emergency Communications Task Force* (ECTF) report calls for a "universal standard/super standard" that provides additional requirements on creation of future data exchange requirements. The super standard was specified to incorporate NIEM, GRA, specifications from the forthcoming NENA Emergency Incident Data Document (EIDD) standard (NENA and APCO, 2013), and information assurance measures (Wisely, Wormeli, and Gabbin, 2013). Future IEPD development should conform to an emerging multilayer framework that includes both the ECTF specifications and the following:

- *base architecture elements*: NIEM, GRA, GFIPM. These should be augmented with true software development kits (SDKs), along with "read this first" tutorials and checklists to help get new developers up to speed quickly.
- *base reference data standard*: There is some debate over which existing standards should be used as the basis for creating this standard; the most common opinion was to use N-DEx as the base, given its role in supporting a nationwide law enforcement data-sharing repository. Again, both the universal standard and base RMS/CAD standard will need SDKs and introductory training material. The base reference is just the first step—a more expansive master data model reference will be needed, as described later.
- *standards testing and certification*: Right now, IJIS Springboard appears to be the de facto standards testing and certification initiative.
- *information assurance*: FBI CJIS policy. This is required now for systems to access law enforcement–sensitive data on the CJIS systems. Given the extent of the cyberthreat, we believe it should become the norm for RMSs and CAD and related systems.

Next steps for IEPD development. Figure 2 summarized which RMS/CAD/other system interfaces are considered critical, as well as which ones had seen at least some development. The ECTF report calls for additional development for 11 interfaces:

- *CAD-related interfaces:*[15] CAD to CAD in another jurisdiction, EMS RMS, EMS Mobile, EOC, Fire RMS, Fire Mobile, Fusion Center, Law Enforcement RMS, Law Enforcement Mobile, and Next-Generation 911.
- *RMS-related interfaces* (besides CAD-RMS): Law Enforcement RMS to Law Enforcement Mobile.

The remaining critical interfaces are Law Enforcement RMS to the following:

- protective order registries
- fusion center systems
- GIS/AVL location (There is also a critical need for a CAD-GIS/AVL interface.)
- license plate readers. (There is also a critical need for a CAD-LPR interface. Note that there is some work going on to create an LPR data-sharing standard.)

We reiterate that the development needs to be compliant with the emerging multilayer framework described above, to avoid overlaps and conflicts.

Master data model. To help avoid the technical overlaps and governance problems to date, there will need to be a *master data model* that provides the point of reference on how to share each of the unique data elements that appear in the various interfaces. Standards developers would be required to use the model's rules for common data elements (e.g., "name" and "address"). Creating new variants building from these common data elements would be allowed, but developers would need to describe how to generate the common data element from their variant.[16] The sponsor should be one or more of the sponsors of the emerging multilayer framework (Global Justice Information Sharing Initiative, NIEM, IJIS, APCO).

Based on interviews regarding what is most important to standardize first, we recommend starting the master model with core *entities* and *descriptors*. The entities are the "objects" of law enforcement data—people, places, things, and events.[17] Core descriptors include name, address, phone numbers, geospatial coordinates, time/dates, and incident-type labels.

Governance Recommendations

Improvement of requirements-generation processes. Gathering and understanding requirements for RMSs, and CAD and other key systems has been a problem area, with practitioners criticizing developers for products that do not meet their needs, developers criticizing practitioners for not properly specifying requirements, and practitioners criticizing developers for the presumption that operators can provide technical requirements. A number of articles have specified problems in working with stakeholders to generate technical requirements, noting problems with operators and developers not speaking the same language, understanding key issues and requirements in their domain but not in the other domain (i.e., knowing what is operationally feasible vs. what is technically feasible), having tacit knowledge that is obvious to one group but not the other, and so on (e.g., Davis, 1982; Valusek and Fryback, 1987; Christel and Kang, 1992). There is, therefore, a need to develop and disseminate requirements generation business processes that can better bridge the gaps between practitioners and developers. Core elements of the process might include:[18]

- building profiles of law enforcement practitioners in different agency roles, taking them through structured interviews that ask:
  - what they do on a typical day
  - what they do during emergency or stressed conditions
  - what works well and what are key problems in both situations
  - what sorts of information they need during routine and stressed conditions, and with what attributes
  - what works well and what needs improvement about what they have now.
- periods of observation in which developers see law enforcement practitioners in different roles at work and can ask them why they are doing what they are doing, to gain a better understanding of what they might need, technologically
- demonstrations in which developers show practitioners examples of different types of displays with different types of information and get feedback. A related approach is to show practitioners lists of common information exchange and display needs (expressed in operational terms; Figures 1–3 are initial examples) and get feedback on how those needs should be modified.
- capturing key takeaways from all of the above, developing a consolidated list of operational needs and corresponding technical requirements.

It is important that findings regarding operational activities and needs be shared across the development community, to avoid technical providers having to find the same core operational understandings repeatedly. This implies funding studies to carry out structured interviews and periods of observation in order to develop common sets of operational needs and contexts for criminal justice information, building on the earlier functional standards.

Fostering the dissemination and widespread use of information-sharing technologies. There is a strong need to go beyond the current piecemeal usages of information-sharing technologies—which are often described as "pilots," "experiments," "demonstrations," and so on—into widespread fielding. Approaches to help meet this need include:

- setting widespread fielding of key information-sharing technologies as a strategic objective. While pilots, experiments, limited tests, and demonstrations continue to be important, especially for emerging technologies, government and commercial focus needs to start moving toward fostering widespread dissemination of mature information-sharing technologies, such as the core NIEM framework and GRA.
- conducting knowledge management and dissemination about key information-sharing technologies—including technical, operational, policy/governance, and acquisition/business model elements—in ways designed for widespread fielding. The key need is to be able to provide information to a large number of developers, practitioners, and executives in a well-organized way that starts with introducing the technologies and ends with all the guidance needed to adapt them quickly. The latter needs to include both detailed technical reference material and development tools (e.g., the aforementioned SDKs and testing tools), as well as detailed policy and procedures material. The educational material needed should build off of existing technical references and case studies, but is just the start of producing a coherent curriculum for information-sharing and safeguarding, as well as mechanisms for delivering it (e.g., portals, e-learning sites).
- determining and employing business model incentives to encourage the use of key information technologies. Model policy and RFP language will be a key part of this, as described below.

Business Model Recommendations

Further development of model policy and RFP language. Beyond the near-term provisions discussed above, we recommend the further development and formalization of model policy and RFP language. These materials should be written at the same level of detail as current model departmental policies—such as those in the IACP's Model Policy Library (IACP National Law Enforcement Policy Center, 2014)—clearly specifying the default for what should be done and asked of vendors to share information. Elements of these materials should include:

- compliance with the emerging multilayer framework and, at a minimum, all relevant critical interfaces as described in Figure 1, including:
  - *federal systems*: NCIC, N-DEx, NIBRS, UCR, IAFIS/NGI
  - *regional and state systems*: whatever is used in the relevant region (including specified NLETS services)
  - *CAD to*: CAD in another jurisdiction, EMS RMS, EMS Mobile, EOC, Fire RMS, Fire Mobile, Fusion Center, Law Enforcement RMS, Law Enforcement Mobile, Next-Generation 911, GIS/AVL, LPR, and Courts Management System
  - *Law Enforcement RMS to*: Law Enforcement Mobile, Protective Order Registries, Fusion Center Systems, GIS/AVL, LPR, Courts Management System, Case Management System, and Jail Management System
  - Standards in the first two dashes above can probably be inserted into standard language now; most of the standards in the third and fourth dashes require further technical development.
- requirements on how compliance will be verified. In the short term, these will have to focus on company-provided tests and references; in the longer term, this should evolve toward formal certification.
- requirements for ensuring RMS/CAD data are easy to export. At a minimum, this includes the ability to export data tables in common text formats, such as comma-separated variables (.csv). It also includes the ability to export geospatial coordinates in latitude-longitude and/or State Plane Coordinate System. Similarly, time and date stamps should be easily interpretable.
- requirements for ensuring that NIEM-compliant IEPD implementations are implemented robustly (no "brittle"

> There is a strong need to go beyond the current piecemeal usages of information-sharing technologies.

instantiations), so that a few localized data errors and inconsistencies will not preclude sharing other data

- compliance with FBI CJIS's information assurance policy, along with any additional information assurance policies considered necessary for that state or region
- language on privacy and civil rights. This should specify defaults on who will have access to specified data, for what purposes, how the usage will be audited, and how long the data should be retained. Special protections should be provided for data that reflect observations of the general public (fixed and mobile cameras, ALPRs). Some efforts to create these policies are under way.

Once these elements are well established, we recommend that DoJ require that federal assistance funds only be spent on systems meeting these criteria, with some flexibility permitted (e.g., which regional and state repositories are required will vary). This has been one of the most-requested provisions across interviews and sessions. The only reason we do not recommend it now is that the framework, standards, and supporting policy are not yet sufficiently mature.

Affordability. We recommend further support for developing SaaS and/or cloud-based models, along with shared and/or regionalized licensing models, and necessary information assurance upgrades, for RMS/CAD systems. While emerging, these do appear promising for providing capability to currently disadvantaged agencies.

Conclusions

Table 2 outlines the major information-sharing issues identified, the recommendations to address them, and key deliverables and other indicators of progress. All are intended to help move agencies from "why can't we know?" to "we do know."

Table 2. Summary of Information-Sharing Issues, Recommendations, and Indicators of Progress

Issue	Recommendation	Indicator of Progress
Technology		
Standards development and usage (such as for IEPDs) must be integrated	• Develop a "super standard" framework for future • Develop remaining critical interface standards • Develop a master data model for key elements of information as part of the super standard	• Super standard developed and disseminated • Critical interface standards developed and disseminated • Master data model developed and disseminated • Compliance testing infrastructure for above developed and disseminated
Governance		
Misunderstandings and knowledge gaps between practitioners and developers are leading to problems with system requirements.	• Develop a common business process for developers to work with practitioners to collectively identify requirements • Share common needs from requirements-gathering efforts to avoid having to find the same requirements repeatedly	• Common business process developed, tested, documented, and disseminated • Common information-sharing needs repository established and populated, and procedures for applying the needs in specific system requirements are published • Volume of users for both common business process and common needs is large
Need to go beyond piecemeal, experimental usage of information-sharing technologies to widespread deployment	• Set widespread dissemination as a strategic objective • Conduct knowledge management and dissemination, providing both practitioners and developers with suitable curriculums from introductions through detailed references	• Dissemination set as a strategic objective in key organizations' strategic plans and there are concrete steps to achieve this objective • Information-sharing educational portals are identified, populated, and managed so as to produce clear curriculums to educate practitioners and developers
Standards development and usage (such as for IEPDs) must be integrated	• Develop a "super standard" framework for future • Develop remaining critical interface standards • Develop a master data model for key elements of information as part of the super standard	• Super standard developed and disseminated • Critical interface standards developed and disseminated • Master data model developed and disseminated • Compliance testing infrastructure for above developed and disseminated
Business Model		
Information-sharing must be properly incentivized and enforced	• Near-term: Develop model policy and acquisition language reflective of the current state of the art in information-sharing • Longer-term: Develop model policy and acquisition language reflective of the mature information-sharing framework and constituent standards • Longer-term: Make funding conditional on compliance with the technical framework and constituent standards described above	• Near-term common policy and acquisition language developed • Long-term common policy and acquisition language developed • Funding made conditional on compliance with the technical framework and conditional standards
More-affordable business models to support the systems sharing information are needed	• Develop and mature SaaS and cloud models for RMS/CAD and other key law enforcement IT • Develop and mature subscription, shared, and regionalized licensing models for key law enforcement IT	• Common business models for SaaS and cloud installations are developed and published • Common business models for subscription, shared, and regionalized licensing models are developed and published

Notes

[1] In this RAND study, representatives from two-dozen agencies were interviewed regarding their most-pressing IT and analytics needs.

[2] As just one example, in 2011 the president of the International Association of Chiefs of Police (IACP) noted during a keynote at the IACP Law Enforcement Information Management conference that his agencies' top priorities were "budget, budget, and budget" (Marshall, 2011). More broadly, a 2010 survey of its members by the Police Executive Research Forum (PERF) found 55 percent of responding departments were "cutting back or eliminating plans to acquire technology" (PERF, 2010, p. 2).

[3] RAND contributed heavily to the Recommendations report (Wisely, Wormeli, and Gabbin, 2013), carrying out much of the analysis leading to the report's specific recommendations. However, the expert practitioners on the task force determined which system-to-system links should be considered critical.

[4] The police department in St. Louis, Mo., was the first to deploy a CAD application in 1965 (McEwen, 2002).

[5] For example, in 1997, Sybase implemented a system linking databases from prosecutors, courts, police, and adult and juvenile corrections through the use of middleware that could transfer information among disparate systems and databases (McKenna, 1998).

[6] Data from CAD systems are often tagged with time and place—additional insights can be discovered when merged with census and other data sources (McEwen, 2002).

[7] These technologies are discussed in more detail in a RAND report on the applicability of future web technologies for criminal justice (Hollywood et al., 2015).

[8] Hanson (2013), for example, refers to the CryptoLocker virus, which encrypts all of a user's files and only decrypts them if the user pays a sizable ransom.

[9] See National Geodetic Survey (January 24, 2013).

[10] See, for example, L. R. Kimball (2011).

[11] Handling police data typically requires logical segregation, physical storage in the United States, encryption at a minimum in transit, prohibition of secondary/commercial use, facilities that can be audited and inspected, an immutable audit log that is easy to query, and vetted personnel.

[12] There are commercial providers who are capable of meeting these requirements and have begun hosting CJIS-compliant data centers (Secure-24, 2012).

[13] Moving core systems into redundant hosted locations can protect operational continuity from large-scale regional disasters (Intrado, 2013).

[14] Descriptions of all of these systems are provided by the FBI (2014).

[15] All of these interfaces are bidirectional; we use "CAD to" or "RMS to" as a way to simplify the discussion, not to imply that these are one-way interfaces.

[16] As an example, suppose a developer wants to create a number of descriptors for robbery events (size of the robbery, type of weapon used, stranger vs. acquaintance robbery, etc.). It should be easy to take these detailed data descriptions and immediately produce a simple "robbery incident" record matching the rules in the master data model.

[17] In the context of the RMS Functional Standard, tags include names, vehicles, property, locations, organizations, and incidents (LEITSC, 2006, pp. 3–5, 8–9).

[18] Example sources for these approaches to requirements analysis include Chemuturi (2013, pp. 33–54) and Masters (2010).

References

Academica Group, "Law Enforcement Perceptions of Cyber Security," Presentation to the 2013 IACP Law Enforcement Information Management Conference, Scottsdale, Ariz., May 22, 2013. As of August 5, 2015:
http://www.theiacp.org/Portals/0/pdfs/LEIM/2013Presentations/2013%20LEIM%20Conference%20Workshop%20-%20Technical%20Track%20-%20State%20of%20LEA%20INFOSEC.pdf

Alaska Law Enforcement Information Sharing System, *Frequently Asked Questions*, undated. As of August 6, 2015:
http://www.aleiss.org/FAQ.htm

ALEISS—*See* Alaska Law Enforcement Information Sharing System.

Andrews, Maxine, *Update on the Alaska Law Enforcement Information Sharing System (ALEISS),* Alaska Law Enforcement Information Sharing System, undated. As of August 6, 2015:
https://www.aleiss.org/ALEISS_Update02022012.pdf

APCO International and IJIS Institute Unified CAD Project Committee, *Unified CAD Functional Requirements*, August 2012. As of August 6, 2015:
https://www.apcointl.org/doc/911-resources/378-unified-cad-functional-requirements/file.html

ARJIS—*See* Automated Regional Justice Information System.

Automated Regional Justice Information System, "What is ARJIS?" ARJIS.org, undated. As of August 6, 2015:
http://www.arjis.org/SitePages/WhatIsARJIS.aspx

Brickley, Dan, and Libby Miller, *The FOAF Project*, January 2014. As of April 10, 2015:
http://www.foaf-project.org/

Chawdry, Rehan, Chris Hellewell, Bruce Kelling, Jim Pingel, and Michael Zurcher, *The Law Enforcement National Data Exchange (N-DEx) Implementer's Trail Guide*, Ashburn, Va.: IJIS Institute, October 2013. As of January 22, 2014:
http://c.ymcdn.com/sites/www.ijis.org/resource/collection/93F7DF36-8973-4B78-A190-0E786D87F74F/CPAC_NDEx-Trail-Guide_20140121.pdf

Chemuturi, Murali, *Requirements Engineering and Management for Software Development Projects,* New York: Springer, 2013.

Christel, Michael, and Kyo C. Kang, *Issues in Requirements Elicitation*, Pittsburgh, Pa.: Carnegie-Mellon University, CMU/SEI Technical Report CMU/SEI-92-TR-012, September 1992.

Crosswind Technologies, *Valcour FAQ,* undated. As of August 6, 2015
http://www.crosswind.com/rms/valcour/valcour-faqs/

Davis, G. B., "Strategies for Information Requirements Determination," *IBM Systems Journal*, Vol. 21, No. 1, 1982, pp. 4–30.

Duval, Dennis, "SaaS Applications Level the Information Sharing Field," *Officer.com,* January 1, 2008. As of August 6, 2015:
http://www.officer.com/article/10249206/saas-applications-level-the-information-sharing-field

Falkenrath, Richard A., "Police Data in the Cloud," *SafeGov,* November 30, 2011. As of August 6, 2015:
http://www.safegov.org/2011/11/30/police-data-in-the-cloud

FBI—*See* Federal Bureau of Investigation.

Federal Bureau of Investigation, *N-DEx: National Data Exchange*, undated. As of January 22, 2014:
http://www.fbi.gov/about-us/cjis/n-dex

———, *The CJIS Security Policy as It Relates to Cloud Computing*, February 2012. As of March 3, 2014:
http://www.safegov.org/media/26301/fbi_statement_on_cjis_and_cloud_feb_2012.pdf

Federal Bureau of Investigation, Criminal Justice Information Services, *Criminal Justice Information Services (CJIS) Security Policy*, Version 5.3, August 4, 2014. As of August 5, 2015:
http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view

Foy, Paul, "John Anthony Borell III, 'Anonymous' Member, Charged in Utah Police Hacking," *Huffington Post*, April 16, 2012. As of January 24, 2014:
http://www.huffingtonpost.com/2012/04/16/john-anthony-borell-iii-anonymous-utah_n_1429106.html

Georgia Tech Research Institute, *GTRI NSTIC Trustmark Pilot*, 2014. As of April 16, 2015:
https://trustmark.gtri.gatech.edu/

Global Standards Council, "Global Standards Package," *Justice Information Sharing,* undated. As of October 15, 2013:
http://it.ojp.gov/GSP

Gordon, John IV, Brett Andrew Wallace, Daniel Tremblay, and John S. Hollywood, *Keeping Law Enforcement Connected: Information Technology Needs for State and Local Agencies*, Santa Monica Calif.: RAND Corporation, TR-1165-NIJ, 2012. As of July 29, 2015:
http://www.rand.org/pubs/technical_reports/TR1165.html

Gortcinsky, Alvin J., and Alec J. Gagne, "Morgan Hill Police Department Downsizes Public Safety Information Sytem," *APCO Bulletin*, 1992. As of October 2013:
http://www.crimestar.com/apcob1992.html

Gould, Jeff, "Los Angeles Pulling the Plug on Gmail at LAPD Is Much Bigger Than You Think," *SafeGov,* December 15, 2011. As of October 2013:
http://safegov.org/2011/12/15/los-angeles-pulling-the-plug-on-gmail-at-lapd-is-much-bigger-than-you-think

———, “FBI Says CJIS Security Rules Are Cloud-Friendly. But Can the Vendors Deliver?” *SafeGov,* February 20, 2012. As of October 2013:
http://safegov.org/2012/2/20/fbi-says-cjis-security-rules-are-cloud-friendly-but-can-the-vendors-deliver

Grimes, Brad, “Big Data Is Taking a Byte Out of Crime,” *FedTech,* October 2013. As of October 2013:
http://www.fedtechmagazine.com/article/2013/10/big-data-taking-byte-out-crime

Hanson, Melissa, “Swansea Police Department Pays Ransom to Computer Hackers,” *Boston Globe*, November 19, 2013. As of January 24, 2014:
http://www.bostonglobe.com/metro/2013/11/19/swansea-police-pay-ransom-open-files-locked-hackers/7bOdi8i7foNkTmdnokMAkP/story.html

Hollywood, John S., Dulani Woods, Richard S. Silberglitt, and Brian A. Jackson, *Using Future Internet Technologies to Strengthen Criminal Justice*, Santa Monica, Calif.: RAND Corporation, RR-928-NIJ, 2015. As of July 29, 2015:
http://www.rand.org/pubs/research_reports/RR928.html

IACP—*See* International Association of Chiefs of Police.

IJIS Institute, “Springboard Pipeline,” IJIS.org, July 26, 2013. As of January 22, 2014 (link no longer active):
http://ijis.org/docs/Springboard_Pipeline_20130726.pdf

International Association of Chiefs of Police, *CAD/RMS*, undated-a. As of February 6, 2014:
http://www.theiacp.org/About-IACP/Governance/-CAD-RMS

———, *Law Enforcement Cyber Center*, undated-b. As of August 5, 2015:
http://www.iacpcybercenter.org/

———, *Procurement*, undated-c. As of January 28, 2014:
http://www.iacptechnology.org/resources/procurement.html

Intrado, *Next Generation 9-1-1: The Essential Guide to Getting Started,* 2013. As of October 2013:
http://www.intrado.com/sites/default/files/documents/NextGen%20 9-1-1%20The%20Essential%20Guide%20to%20Getting%20Started.pdf

Kimball, L. R., *Plan for Next Generation 9-1-1,* NG9-1-1, January 2011. As of October 2013:
http://www.maine911.com/psap/Publications/Maine%20NG911%20 Plan2011l.pdf

Law Enforcement Information Technology Standards Council, *Standard Functional Specifications for Law Enforcement Computer Aided Dispatch Systems*, Alexandria, Va., 2006. As of January 24, 2014:
http://www.theiacp.org/portals/0/pdfs/LawEnforcementCADSystems.pdf

———, *Standard Functional Specification for Law Enforcement Computer Aided Dispatch Systems*, Alexandria, Va., 2008. As of January 24, 2014:
http://www.theiacp.org/portals/0/pdfs/LawEnforcementRMSv2.pdf

———, *A Project Manager’s Guide to RMS/CAD System Software Acquisition*, Alexandria, Va., 2009. As of January 24, 2014:
http://www.theiacp.org/portals/0/pdfs/PMGuide_RMS-CAD_System_Software_Acquisition.pdf

———, *Standard Functional Specifications for Law Enforcement Records Management Systems Version 2*, Washington, D.C.: Office of Justice Programs, 2010.

LEITSC—*See* Law Enforcement Information Technology Standards Council.

Lerman, Julie, “What the Heck Are Document Databases?” *MSDN Magazine*, November 2011. As of April 16, 2015:
https://msdn.microsoft.com/en-us/magazine/hh547103.aspx

Marshall, Mark A., IACP President, “Policing in the 21st Century,” presentation to the IACP Law Enforcement Information Management Conference, San Diego, Calif., June 13, 2011.

Masters, Morgan, “An Overview of Requirements Elicitation,” ModernAnalyst.com, July 7, 2010. As of June 17, 2015:
http://www.modernanalyst.com/Resources/Articles/tabid/115/ID/1427/An-Overview-of-Requirements-Elicitation.aspx

McEwen, Tom, ed., *Computer Aided Dispatch in Support of Community Policing,* Alexandria, Va.: Institute for Law and Justice, July 2002. As of October 2013:
http://www.ilj.org/publications/docs/CAD_Community_Policing_Final_Report.pdf

McKenna, Ed, “High-Tech Crime Fighters: Law Enforcement Officials Add IT to Their Arsenals,” *Washington Technology,* July 17, 1998. As of October 2013:
http://washingtontechnology.com/articles/1998/07/17/hightech.aspx

Micro Focus, *City of Inglewood,* 2011. As of October 2013:
http://www.microfocus.com/assets/city-of-inglewood_tcm6-201481.pdf

Milstead, Michael, “Connect South Dakota Revolutionizes State’s Law Enforcement and Homeland Security Information Sharing,” ISE.gov, February 12, 2013. As of January 24, 2014:
http://www.ise.gov/blog/sheriff-michael-milstead/connect-south-dakota-revolutionizes-state%E2%80%99s-law-enforcement-and

Mitchell, Robert L., “It’s Criminal: Why Data Sharing Lags Among Law Enforcement Agencies,” *Computer World,* 2013. As of October 2013:
http://www.computerworld.com/s/article/9243354/It_s_criminal_Why_data_sharing_lags_among_law_enforcement_agencies_

Morgan, Kenneth E., *Computer Aided Dispatch Technology: A Study of the Evolution and Expectations of CAD and a Comparative Survey of CAD in the U.S. Fire Service and the Clark County Fire Department,* dissertation, University of Nevada, Las Vegas, 2003. As of October 2013:
http://digitalscholarship.unlv.edu/cgi/viewcontent.cgi?article=1575&context=thesesdissertations

National Criminal Justice Association, *Why Can't We Share? The Need to Share Information Electronically Is a National Imperative: Terrorists Could Be Hiding Between the "Information Silos,"* Washington, D.C.: Government Printing, 2004. As of August 5, 2015:
http://www.kms.ijis.org/db/attachments/public/32/1/1-page%20summary.pdf

National Emergency Number Association and the Association of Public-Safety Communications Officials, EIDD Work Group, *NENA/APCO Emergency Incident Data Document (EIDD) Information Document*, Alexandria, Va., NENA/APCO-INF-005, September 24, 2013.

National Geodetic Survey, "SPC Utilities," *National Geodetic Survey*, January 24, 2013. As of February 3, 2014:
https://www.ngs.noaa.gov/TOOLS/spc.shtml

National Information Exchange Model Program Management Office, "NIEM Version 3.1 Is Now Available," NIEM.gov, May 29, 2015. As of August 6, 2015:
https://www.niem.gov/news/Pages/NIEM-version-3-1-is-Now-Available.aspx

National Law Enforcement and Corrections Technology Center, "Info Sharing Comes in from the Cold," *TechBeat*, Fall 2006. As of October 2013:
https://www.justnet.org/pdf/InfoSharing.pdf

National Law Enforcement Telecommunications Center, "What We Do: Transactions," Nlets.org, 2015. As of August 5, 2015:
http://www.nlets.org/about/what-we-do

National Task Force on Interoperability, *Why Can't We Talk? Working Together to Bridge the Interoperability Gap to Save Lives,* Washington, D.C.: National Institute of Justice, 2005.

NCJA—*See* National Criminal Justice Association.

NENA—*See* National Emergency Number Association.

New World Systems, "New World Systems' Solutions Help the Northeast South Dakota Rural Information Exchange Combat Crime and Drugs," press release, September 28, 2013. As of January 24, 2014:
http://www.policeone.com/police-products/investigation/drug-enforcement-software/press-releases/2720097-New-World-Systems-Solutions-Help-the-Northeast-South-Dakota-Rural-Information-Exchange-Model-RIEM-Combat-Crime-and-Drugs/

NIEM—*See* National Information Exchange Model.

NLETS—*See* National Law Enforcement Telecommunications System.

Office of Justice Programs, *Global Federated Identity and Privilege Management*, U.S. Department of Justice, undated-a. As of August 6, 2015:
http://www.it.ojp.gov/initiatives/gfipm

———, *IEPD Clearinghouse*, U.S. Department of Justice, undated-b. As of October 15, 2013:
http://it.ojp.gov/framesets/iepd-clearinghouse-noClose.htm

———, *Justice Information Sharing*, U.S. Department of Justice, undated-c. As of January 8, 2014:
https://it.ojp.gov/default.aspx

OJP—*See* Office of Justice Programs.

Ott, Michael, and Aaron Gorrell, "CAD/RMS Implementation in Palm Beach County Sheriff," presentation to the 2013 IACP Law Enforcement Information Management Conference, Scottsdale, Ariz., May 22, 2013. As of January 24, 2014:
http://www.theiacp.org/Portals/0/pdfs/LEIM/2013Presentations/2013%20LEIM%20Conference%20Workshop%20-%20Technical%20Track%20-%20CADRMS%20Implementation.pdf

Parker, Scott, and Steve Wisely, *Priority Data Exchanges for Local Communications Centers: A List of Data Exchanges Relating to Computer Aided Dispatch Systems*, Asheville, Va.: IJIS Institute and Association of Public Safety Communications Officials–International, 2009.

PERF—*See* Police Executive Research Forum.

PM-ISE—*See* Program Manager, Information Sharing Environment.

Police Executive Research Forum, *Is the Economic Downturn Fundamentally Changing How We Police?* Critical Issues in Policing Series, Vol . 16, Washington, D.C.: Police Executive Research Forum, 2010.

Policesoftware.com, homepage, undated. As of October 2013:
http://www.policesoftware.com

Porter, Scott, "CAPSIT—OpenRMS," Presentation to the 2007 Government Open Source Conference (GOSCON), Portland, Ore., October 15, 2007a. As of August 6, 2015:
https://media.oregonstate.edu/media/t/0_d6jtbkzu

———,*The OpenRMS Project: A Case Study in Free Software for Government,* 2007b. As of August 6, 2015:
http://site07.goscon.org/files/goscon.org/presentation/Mon-915-Porter.pdf

Program Manager, Information Sharing Environment, *Project Interoperability*, undated. As of June 10, 2015:
http://project-interoperability.github.io/

Regional Information Sharing Systems, "RISS Overview," RISS.net, undated. As of August 5, 2015:
https://www.riss.net/Default/Overview

Secure-24, *Law Enforcement in the Cloud: InterAct Gains Efficiencies, Meets Compliance Requirements,* 2012. As of August 6, 2015:
http://www.secure-24.com/wp-content/uploads/2015/03/Law-Enforcement-Case-Study.pdf

Standards Coordinating Council, *Standards*, 2015. As of June 10, 2015:
http://www.standardscoordination.org/standards

Tiburon Inc., East Hampton Police Move CAD/RMS Solution to the Cloud Reducing Costs and Complexity, September 2012. As of August 6, 2015:
http://cdn.agilitycms.com/tiburon/Documents/MSFT-TE-TownEastHampton-Case-Study-v2012-09-25.pdf

Unified CAD Project Committee, *High Priority Information Sharing Needs for Emergency Communications and First Responders*, Ashburn, Va.: IJIS Institute and Association of Public Safety Communications Officials–International, 2012.

Valusek J. R, and D. G. Fryback, Information Requirements Determination: Obstacles Within, Among and Between Participants," in R. Galliers, ed., *Information Analysis: Selected Readings*, Reading, Mass.: Addison Wesley, 1987, pp. 139–151.

Wisely, Steve, Paul Wormeli, and Donald Gabbin, *Recommendations of the Emergency Communications Task Force*, Ashburn, Va.: IJIS Institute and Association of Public Safety Communications Officials–International, 2013.

Wyllie, Doug, "SaaS Technology Helps Mid-Sized Ky. PD Fight Crime," *PoliceOne,* Feb. 23, 2013. As of October 2013:
http://www.policeone.com/chiefs-sheriffs/articles/2008711-SaaS-technology-helps-mid-sized-Ky-PD-fight-crime/

About the Authors

John S. Hollywood is a senior operations researcher at the RAND Corporation and a professor of policy analysis at Pardee RAND Graduate School. His principal focus is information systems research in support of improving security, ranging from crime prevention to terrorism prevention to improving combat effectiveness. His recent research projects have included examinations of predictive policing, high-priority information technology needs for law enforcement, and U.S. effectiveness at foiling terror plots.

Zev Winkelman is a core faculty member at the Pardee RAND Graduate School and an associate information scientist at RAND specializing in big data analytics, social media, and cyber security. He has more than 15 years of experience in computer engineering and software development including a master's degree in forensic computing and counterterrorism.

About This Report

Law enforcement agencies—and first responders in general—depend heavily on core information technology (IT) systems known as records management systems (RMSs) and computer-aided dispatch (CAD) systems. Increasingly, agencies need capabilities that require interoperability among RMSs and CAD and other agency, local, state, and federal systems. Access to these new capabilities requires systems that are reasonably affordable and maintainable, especially given highly constrained budgets. This report examines high-level needs for, and barriers to, RMS/CAD interoperability and accessibility. It also identifies some promising approaches that, with further development, might help overcome these barriers. It should be of interest to law enforcement practitioners, systems developers, and associations and policymakers responsible for directing standards and policies regarding RMSs and CAD and other key law enforcement systems.

This work was conducted by the National Law Enforcement and Corrections Technology Center of Excellence on Information and Geospatial Technology at the National Institute of Justice (NIJ). This guide will be of interest to law enforcement personnel at all levels and is one in a series of NIJ-sponsored resources for police departments.

The authors would like to acknowledge the valuable contributions of the reviewers of this report, Edward Balkovich and Rui Chen, as well as project sponsors Steve Schuetz and Bill Ford of the National Institute of Justice. The research reported here was conducted in the RAND Safety and Justice Program, which addresses all aspects of public safety and the criminal justice system, including violence, policing, corrections, courts and criminal law, substance abuse, occupational safety, and public integrity. Program research is supported by government agencies, foundations, and the private sector.

This program is part of RAND Justice, Infrastructure, and Environment, a division of the RAND Corporation dedicated to improving policy and decisionmaking in a wide range of policy domains, including civil and criminal justice, infrastructure protection and homeland security, transportation and energy policy, and environmental and natural resource policy.

Questions or comments about this report should be sent to the project leader, John Hollywood (John_Hollywood@rand.org). For more information about the Safety and Justice Program, see http://www.rand.org/safety-justice or contact the director at sj@rand.org.

NIJ | National Institute of Justice
STRENGTHEN SCIENCE. ADVANCE JUSTICE.

This publication was made possible by Award Number 2010-IJ-CX-K007, awarded by the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice. The opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect those of the Department of Justice.

Limited Print and Electronic Distribution Rights

www.rand.org

RAND CORPORATION

The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest.

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors. **RAND**® is a registered trademark.