NISTIR 8255

Interoperability of Real-Time Public Safety Data: Challenges and Possible Future States

Britta Voss
Eric Anderson

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8255

National Institute of Standards and Technology
U.S. Department of Commerce

NISTIR 8255

Interoperability of Real-Time Public Safety Data: Challenges and Possible Future States

Britta Voss
Eric Anderson
Public Safety Communications Research Division
Communications Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8255

June 2019

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Undersecretary of Commerce for Standards and Technology

National Institute of Standards and Technology Interagency or Internal Report 8255
Natl. Inst. Stand. Technol. Interag. Intern. Rep. 8255, 90 pages (June 2019)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8255

Executive Summary

The growth of broadband wireless networks and associated data sharing technologies presents a unique opportunity for the public safety community to revolutionize the operational capabilities of their communication technologies. In particular, the creation of a unified national public safety broadband network (NPSBN) creates the potential for more seamless cross-agency information sharing than was possible with legacy networks tied to specific jurisdictions. However, achieving a state of interoperable, real-time, cross-agency data sharing will require tackling key technical limitations, economic constraints, and a lack of governance resources. This report summarizes these challenges and draws from examples in public safety and beyond to propose actions for public safety leaders to accelerate the transition to a more interoperable data sharing environment.

This report is intended to inform and motivate public safety leaders to create the conditions that will allow first responders to derive maximum operational benefits from the capabilities provided by emerging technologies and the NPSBN. However, developing the technical, economic, and governance structures that are needed to revolutionize data sharing technology use for public safety likely cannot be accomplished by individual agencies working in isolation. Therefore, this report also serves to encourage technology developers to support more interoperable data sharing technologies for public safety and provides recommendations for funding bodies and federal partners to support multi-agency, cross-jurisdiction data sharing initiatives.

We assessed current challenges to data sharing interoperability in three areas:

Technical Challenges

- Existing public safety data exchange standards have limited scope and have not been widely adopted by technology developers.
- The lack of a federated public safety identity, credentialing, and access management solution prevents data sharing technologies from providing inter-agency interoperability, even if technologies use standardized data.

Economic Challenges

- Proprietary end-to-end data sharing solutions discourage data interoperability by providing multiple functionalities in a siloed system and encouraging vendor lock-in.
- Modular, standardized solutions would allow agencies to choose the collection of functionalities that best suits their needs while still supporting real-time cross-agency interoperability.
- Community consensus on baseline data sharing functionalities would provide technology developers with guidance on developing products with an appropriate balance of interoperable and proprietary features.

Governance Challenges

- Agencies need to make careful decisions about the who, what, where, when, why, and how of data sharing *before* a multi-agency incident occurs.
- Agencies can draw knowledge and inspiration for data sharing policies from initiatives in related domains and from local experts like city and state chief information officers.
- Standardized, pre-defined templates for policies, contracts, and requests for proposals are needed to decrease the burden for individual agencies adopting data sharing technologies.

Based on the data sharing interoperability challenges facing the public safety community and the relevant data sharing frameworks assessed in this report, we identified five steps agencies can embark on now to accelerate data sharing interoperability.

Recommended near-term public safety agency actions:

1. **Leverage Request for Proposal (RFP) requirements.** Be as specific as possible in RFP and contract language about the interoperability requirements and specifications of data sharing technologies, including data exchange standards where appropriate. Reference guidance from relevant bodies such as SAFECOM and the National 911 Program.
2. **Participate in Identity, Credentialing, and Access Management (ICAM) solution development.** Provide practitioner expertise on features and requirements for the SAFECOM ICAM working group and other bodies studying and developing federated identity management and access control approaches for public safety data systems. As soon as possible, include such tools in RFP and contract interoperability requirements.
3. **Develop inter-agency data sharing partnerships.** Build inter-agency commissions, task forces, working groups, etc., charged with identifying the agencies' collective data sharing interoperability goals, model use cases, requirements, and benchmarks of success. These bodies can build the foundation for a public safety-wide data sharing strategy.
4. **Collaborate with the broader public safety community.** Extend the influence and knowledge base of regional task forces by engaging with national and international public safety entities, including state and federal bodies, practitioner organizations, research groups, industry groups, standards developing organizations, and others.
5. **Make the case for investments in data sharing.** Leverage existing monitoring and evaluation data to analyze agency data use and data sharing patterns. Agency leaders can use such analyses to make evidence-based arguments regarding future investments in data sharing resources.

In parallel to the actions taken by individual agencies, the entire public safety community can make significant progress towards an interoperable future for real-time data sharing technologies. We identified two key actions that will be critical to achieving this goal.

Community Recommendation 1: Prioritize funding for data integration tools and data sharing governance work

Data sharing initiatives must not become an unfunded mandate. Material support is particularly needed for the development of tools that integrate and convert data from a variety of sources into specific open formats and the logistical costs of participating in data sharing governance activities.

Community Recommendation 2: Establish a community-wide public safety data sharing task force to develop governance resources and a framework for data sharing interoperability requirements

Making transformational progress on data sharing interoperability requires leadership from a group composed of trusted leaders and experts in the public safety technology field, spanning disciplinary and jurisdictional boundaries. This body would be tasked with developing template language for data sharing policies, requests for proposals, and contracts, as well as developing a public safety data sharing framework including baseline data elements, data exchange standards, and reference implementations. These resources would facilitate agencies large and small in realizing the benefits of data sharing technologies without having to reinvent the wheel to make procurement, policy, and conformance testing decisions.

Abstract

The proliferation of advanced data sharing technologies and the emergence of a national public safety broadband network (NPSBN) are revolutionizing the communications capabilities of first responders in the United States. Fire departments, law enforcement agencies, emergency medical service providers, and other public safety entities are beginning to adopt messaging applications, sensors, networked cameras, and other technologies that provide a wealth of real-time information about people, infrastructure, and incident environments. However, the rapid expansion of these technologies presents important technical, economic, and governance challenges that need to be addressed for these technologies to provide interoperable communication solutions for all members of the public safety community. This report provides an overview of these challenges, focusing on interoperability implications of data exchange standards, data access control approaches, and data sharing policy frameworks. It explores the limitations of efforts to improve the interoperability of data sharing technologies to date and provides recommendations for the public safety community to leverage existing resources and organizations and build new alliances to promote a more interoperable future for data sharing technologies. The report is intended to inform and motivate public safety leaders to create the conditions that will allow first responders to derive maximum operational benefits from the capabilities provided by emerging technologies and the NPSBN, and to encourage technology developers to support more interoperable data sharing technologies for public safety.

Keywords

data sharing; emergency management; governance; information sharing; interoperability; public safety; standards.

Table of Contents

List of Tables

List of Figures

Glossary

3GPP	Third Generation Partnership Project
ABAC	Attribute-Based Access Control
ABE	Attribute Based Encryption
ACL	Access Control List
ADM	Agency Data Manager
AED	Automatic External Defibrillator
APCO	Association of Public-Safety Communications Officials-International
AUVSI	Association for Unmanned Vehicle Systems International
BayRICS	Bay Area Regional Interoperable Communications System
CAD	Computer-Aided Dispatch
CAP	Common Alerting Protocol
CIO	Chief Information Officer
CJIS	Criminal Justice Information Services
DHS	U.S. Department of Homeland Security
EDXL	Emergency Data Exchange Language
EIDD	Emergency Incident Data Document
EIDH	Emergency Incident Data Hub
EMAC	Emergency Management Assistance Compact
EMS	Emergency Medical Services
FEMA	U.S. Federal Emergency Management Agency
FOIA	Freedom of Information Act
FRNA	First Responder Network Authority
GIS	Geographic Information System
HIPAA	Health Insurance Portability and Accountability Act
HL7	Health Level 7 International
IACP	International Association of Chiefs of Police
IAFC	International Association of Fire Chiefs
IAEM	International Association of Emergency Managers
IC	Incident Commander
ICAM	Identity, Credentialing, and Access Management
IEC	International Electrotechnical Commission
IFRC	International Federation of Red Cross and Red Crescent Societies
IJIS	Integrated Justice Information Systems
IoT	Internet of Things
IPAWS	Integrated Public Alert and Warning System
IP	Internet Protocol
ISA IPC	Information Sharing and Access Interagency Policy Committee
IT	Information Technology
JHU APL	Johns Hopkins University Applied Physics Lab
JSON	JavaScript Object Notation
LA-RICS	Los Angeles Regional Interoperable Communications System
LMR	Land Mobile Radio
LTE	Long-Term Evolution
MCFD	Marion County Fire Department

MCV	Mission-Critical Voice
MDT	Mobile Data Terminal
MMS	Multimedia Messaging Service
MOU	Memorandum of Understanding
MWCOG	Metropolitan Washington Council of Governments
MWAA	Metropolitan Washington Airports Authority
NASEMSO	National Association of State EMS Officials
NASNA	National Association of State 911 Administrators
NCCoE	National Cybersecurity Center of Excellence
NCIC	National Crime Information Center
NCRnet	National Capital Region Network
NCSWIC	National Council of Statewide Interoperability Coordinators
NENA	National Emergency Number Association
NGAC	Next Generation Access Control
NG911	Next Generation 911
NIEM	National Information Exchange Model
NIMS	National Incident Management System
NISC	National Information Sharing Consortium
NIST	National Institute of Standards and Technology
NITRD	Networking and Information Technology Research Directorate
NFPA	National Fire Protection Association
NPSBN	National Public Safety Broadband Network
NPSTC	National Public Safety Telecommunications Council
OASIS	Organization for the Advancement of Structured Information Standards
OGC	Open Geospatial Consortium
ONC	Office of the National Coordinator
ONVIF	Open Network Video Interface Forum
OSAC	Organization of Scientific Area Committees
RBAC	Role-Based Access Control
REMS	Riverside Emergency Medical Services
RFD	Riverside Fire Department
RFP	Request for Proposals
PBAC	Policy-Based Access Control
PCII	Protected Critical Infrastructure Information
PII	Personally Identifiable Information
PM-ISE	Program Manager for the Information Sharing Environment
PSAP	Public Safety Answering Point
PSCR	Public Safety Communications Research
SCBA	Self-Contained Breathing Apparatus
SDO	Standards Developing Organization
SIEC	Statewide Interoperability Executive Committee
SIGB	Statewide Interoperability Governing Body
SPOC	Single Point of Contact
SMS	Short Message Service
SVRDT	Silicon Valley Regional Data Trust
SWIC	Statewide Interoperability Coordinator

TIC	Thermal Imaging Camera
UAS	Unmanned Aircraft System
vUSA	Virtual USA
WGS84	World Geodetic System 1984
WMATA	Washington Metropolitan Area Transit Authority
XACML	eXtensible Access Control Markup Language
XML	Extensible Markup Language

1. Introduction

Effective decision-making requires access to timely and relevant data. The explosion of data-driven technologies such as high-precision mapping and powerful data analytics, accelerated by the expansion of high-speed internet access and ubiquitous computing and storage capabilities, creates an immense opportunity for the public safety community to leverage powerful analytical tools for improved mission-critical decision-making. However, to make the firehose of data potentially available to first responders timely, relevant, and usable, public safety agencies and technology developers need to collectively address the technical, economic, and governance challenges which currently threaten the beneficial use of broadband-enabled data sharing technologies for emergency response. This report presents the obstacles facing public safety agencies and technology developers in creating and adopting useful data sharing solutions, use cases which highlight how truly interoperable mission critical data sharing could advance the capabilities of first responders and those who support them, and possible approaches towards achieving such a future for public safety data sharing.

In the public safety arena, "data" has traditionally been restricted to data which are available over land mobile radio (LMR) systems, including data transmitted via computer-aided dispatch (CAD) systems and retrieved from centralized sources such as state license plate registration databases or federal criminal history records. Access to such data is sometimes only possible from a police, fire, or emergency medical services (EMS) station via computers or phone calls or through radio to Internet Protocol (IP) interfaces, but it is increasingly being deployed for use in the field through communications center personnel over the radio or mobile data terminals (MDT). Public safety agencies equipped with MDTs in their vehicles typically have access to incident data, but emerging technologies for sharing large quantities of text, geospatial, video, and other data types offer vastly greater capabilities.

In recent years, the growth of reliable mobile internet connectivity across most of the United States through commercial broadband data networks has given customers instantaneous access to a huge quantity and variety of data from nearly any location. Services running on broadband data networks can provide first responders with the ability to share raw data, such as text messages, images, or building plans, as well as intelligence generated from the analysis of one or multiple data sources to increase the safety of members of the public and responding personnel [1]; some agencies are already utilizing these tools. For example, a collection of sensors worn by firefighters could trigger alerts to the firefighters and their incident commander if a firefighter's heart rate exceeds a user-specific threshold. Or by analyzing multiple data streams, an artificial intelligence system could dynamically optimize the distribution of personnel and resources during a natural disaster response.

"Data sharing" in this document refers to (1) the transmission of data that are used in emergency incident response among first responders and second responders[1] (active), or (2) the provision of access to data stored on devices, servers, or cloud repositories (passive). The potential value of such capabilities grows as more agencies are able to participate in data sharing. As an incident grows in scale and complexity, integrating new agencies and personnel into the response becomes more challenging, and lack of interoperability between communications systems can result in slow and uneven distribution of information to the people and agencies who need it (Fig. 1).

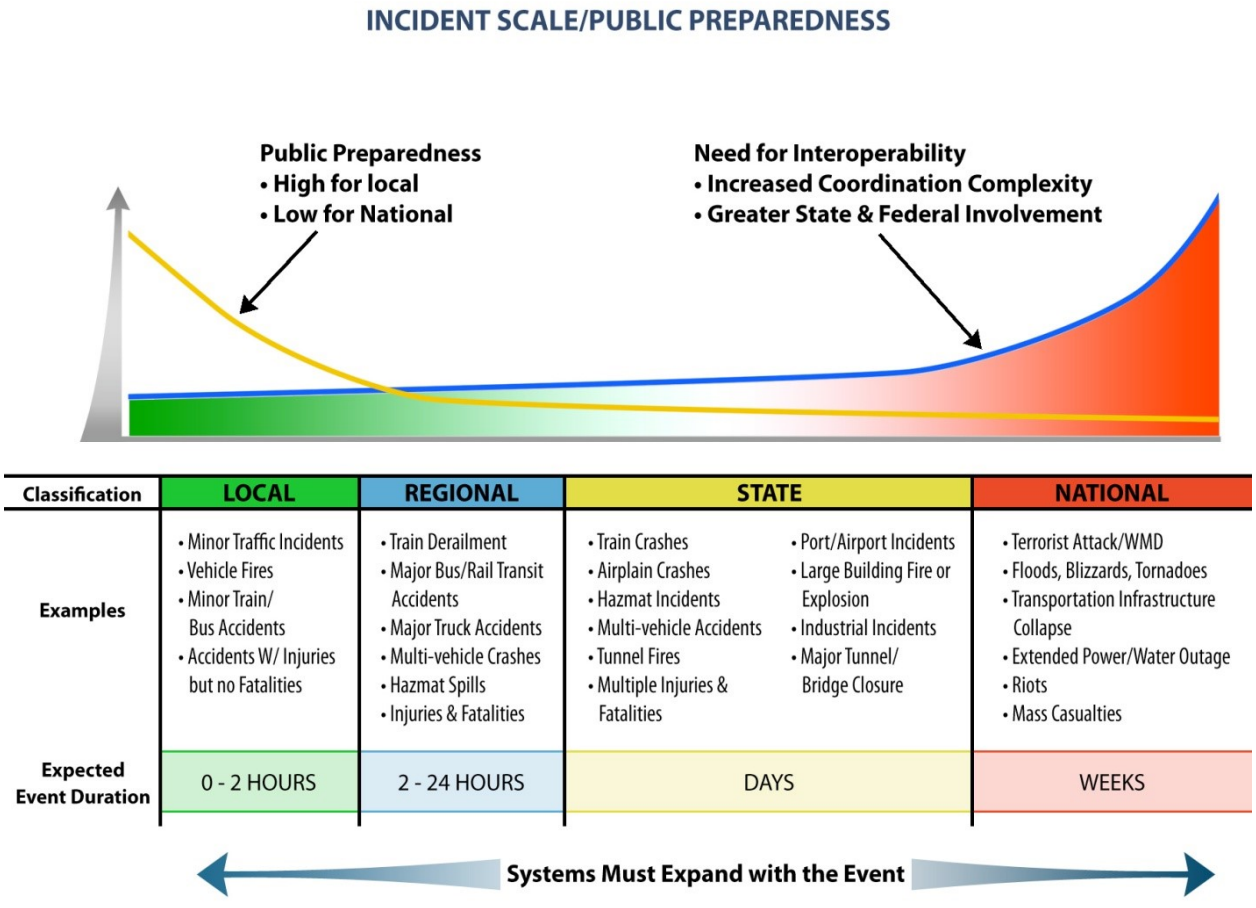


Fig. 1. Incident scale and interoperability needs

The need for communications interoperability and cross-jurisdictional coordination increases as incident scale and complexity increases. Reproduced from Ref. [2].

In the most basic sense, "interoperability" can mean nothing more than the ability to send bits of data from one system to another. However, in practice, **interoperability between disparate systems requires highly structured data exchange procedures (i.e., standards)**

[1] "Second responders" refers to non-public safety entities which can participate in emergency response, including other public agencies, businesses, non-governmental organizations, and members of the public.

that ensure that data sent by one system can be interpreted and used by a receiving system [3]. The latter type of interoperability is necessary for cross-agency data sharing given the wide variety of technical architectures and products being used in public safety communication systems today. Furthermore, *real-time* cross-agency data sharing will require a greater degree of interoperability in how first responders control access to data than currently exists.

Data sharing can be conceptualized in two dimensions: the data sharing process and the data sharing system. In the data sharing process view, the movement of data begins with capture and ends with long-term storage, with numerous intermediate steps including encoding, compression, transmission, broadcasting, visualization, alerting, triage, and forensics (Fig. 2). Each step along this process requires interoperability, security, and policy considerations, especially if the data are shared beyond the entity that captured the data. For practical reasons, data integration tools may only address a subset of steps in the process or types of data, but every data source potentially passes through each step of the process.

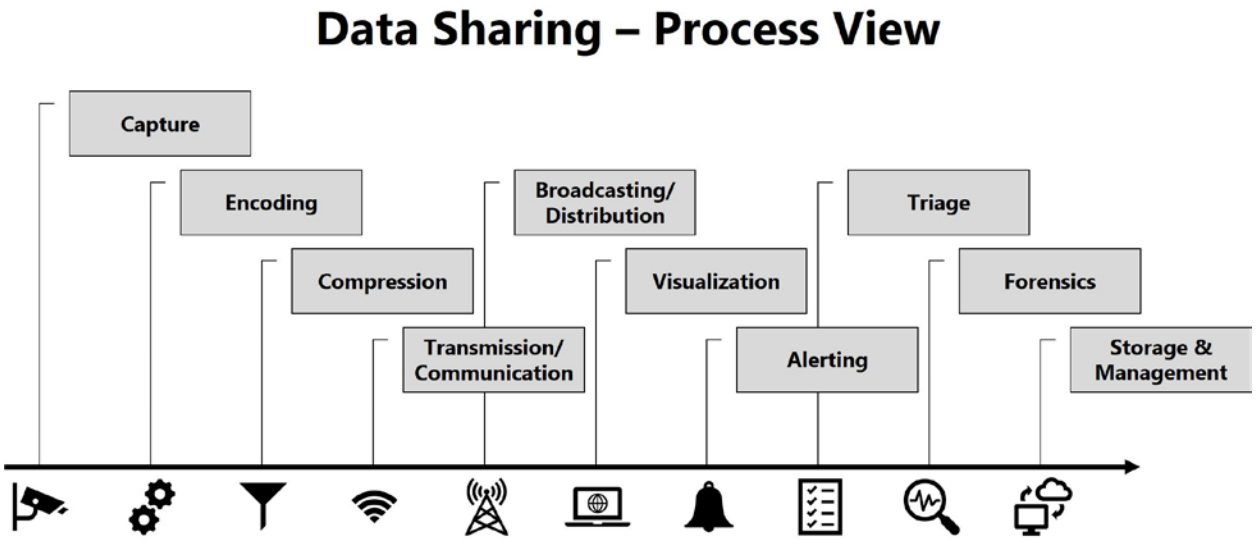


Fig. 2. Steps in the data life cycle

The data sharing lifecycle includes distinct stages, each with important interoperability, security, and policy considerations. Adapted from the 2016 Video Analytics in Public Safety workshop report's "major public safety workflow components" [4].

In the data sharing system view, individual public safety agencies and related entities operate in a layered jurisdictional environment including local, regional, state, federal, and potentially other authorities (Fig. 3). While responding to an incident, a first responder or device affiliated with a particular agency may share data with individuals or devices from an agency or other entity under different jurisdictional authorities. The nature of the entities sharing data, as well as the type of data and the locality in which the data was captured, transmitted, and stored, can all influence the policies governing how the data are shared. For example, sharing of personally identifiable information (PII) or protected health information

may be governed by laws and policies at every level of governmental authority, as well as privacy policies of technology providers and individual agencies.

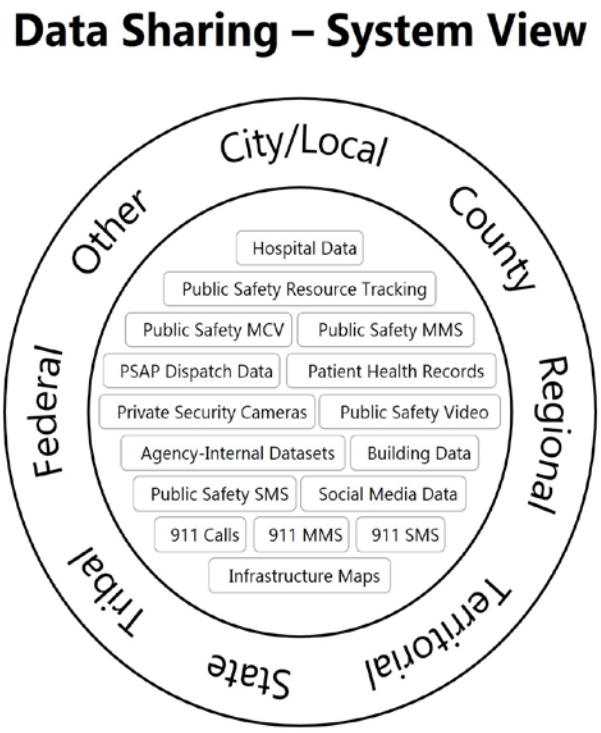


Fig. 3. Layers of authority affecting data sharing

Multiple layers of authority can apply to data shared between agencies under different jurisdictions or legal/policy obligations.

Consider the following scenario describing an incident where an agency has immediate access to a variety of real-time data sources, and can seamlessly extend data access to additional first responders as the circumstances evolve:

> *A fire department responds to an automated alarm at a large office building. Before arriving at the incident, the department instantly accesses the fire panel information and a virtual fire control room, which visualizes streaming video from the building's security cameras, details about the building's construction, 3-D locations of all first responders and the 911 caller(s), and digital maps of the building's interior with overlays of temperature data, exit pathways, key boxes, and other features. This information helps the fire department activate the appropriate response prior to arriving on-scene. The department also immediately accesses numerous external data sources to visualize the building's utility connections (water, electricity, natural gas), traffic information for the route to the incident, and the status of nearby public safety resources (e.g., unmanned aerial systems, hazardous materials response teams) that may need to be called upon. At the incident, the fire department learns from*

evacuated occupants that an individual inside the building may have a weapon and is acting erratically. The fire department reports this information and summons the nearest law enforcement unit for support, immediately providing the officers and communications center personnel with access to the building's security cameras, floor plans, and other incident data.

In such a scenario, the ability to immediately access data sources which are not administered by the agency itself, and to share data with other agencies on the fly, is critical to effectively responding to the incident. Emerging data sharing technologies currently lack the technical standardization and inter-agency governance structures to ensure such cross-agency interoperability. While full system interoperability requires solutions that span the entire data life cycle (Fig. 2), this report focuses primarily on aspects of interoperability that have not been addressed by standards bodies or require unique considerations for real-time public safety use cases, and therefore represent the areas of greatest need and opportunity for making significant progress. Public safety information sharing platforms that have been adopted already such as messaging applications[2] and situational awareness dashboards are generally not capable of exchanging mutually intelligible real-time data with other platforms[3]. **While agencies are in the early stages of adopting advanced data sharing capabilities, the time is ripe for the public safety community to collectively consider the possible approaches to solving this challenge and chart a path towards a desired future state.**

Each major section of this report (including the use cases in Appendix A) is followed by a brief summary of key takeaways to help readers navigate the major concepts and find the sections of greatest interest to their role or agency.

Introduction: Key Takeaways.

- In recent years, public safety data sharing has expanded far beyond the capabilities of agency databases and CAD and MDT systems to include text, image, video, geospatial, and other types of data and analytics products derived from public safety agencies, other supporting agencies and organizations, private companies, and the public.

[2] Unless otherwise specified, the word "application" is used in this document in a general way, meaning a use or purpose for a product or approach. When a different meaning is intended, more specific terms are used, such as software application, mobile application, or the abbreviation "app."

[3] For example, the mobile applications employed by Harris County at the Super Bowl LI pilot each provided stand-alone functionality, even though some apps generated the same types of data [5]. Likewise, different mutual aid systems demonstrated at the 2017 National Mutual Aid Technology Tabletop Exercise were not able to share situational awareness data with each other [6]. If such systems were interoperable with respect to data exchange, then two platforms/apps generating data of the same type (e.g., geospatial, video, images, etc.) would be capable of ingesting and using the corresponding data from outside platforms/apps.

- The criticality of data sharing interoperability increases as incident scale and complexity grow.
- Data interoperability considerations are needed at all stages of the data life cycle, from collection to long-term storage, and at various levels of authority, from local to federal.
- Achieving real-time, cross-agency data sharing interoperability requires a community-wide strategy to effectively address technical, economic, and governance challenges simultaneously.

2. Methodology

The information presented in this report derives from a combination of literature research and discussions with subject matter experts and personnel in the public safety community. We drew from white papers and reports published by the First Responder Network Authority (FRNA), the U.S. Department of Homeland Security (Emergency Communications Division and Science and Technology Directorate), the National Public Safety Telecommunications Council (NPSTC), and the Integrated Justice Information Systems (IJIS) Institute as a foundation for previous standardization efforts in the public safety sector and principles for information sharing governance. We also reviewed documentation for data exchange standards from the Organization for the Advancement of Structured Information Systems (OASIS), the National Emergency Number Association (NENA), the Association of Public-Safety Communications Officials-International (APCO), the National Information Exchange Model (NIEM), the National Fire Protection Association (NFPA), the Federal Emergency Management Agency (FEMA) Integrated Public Alert and Warning System (IPAWS), and other standards developing organizations (SDOs) and technical bodies. After action reports from technology implementation pilots and tabletop exercises provided context for current technology capabilities and realistic public safety use cases. Numerous conversations with experts from technical and practitioner backgrounds provided critical context and detail to our understanding of the current state and future vision of public safety data interoperability. Specific contributors are identified in the Acknowledgements.

3. Challenges of seamless real-time data sharing

In a perfect world, all stakeholders utilizing components of the emergency communications ecosystem would have the ability to share information across discipline and jurisdictional boundaries during mutual aid incidents while ensuring appropriate control on exactly who received what data without diverting their time or attention to managing the flow of information. Technological and policy obstacles to seamless real-time information sharing can degrade optimal first response in emergency situations [7]. At the same time, the available solutions to these obstacles can present a financial obstacle to under-resourced

public safety agencies. While the public safety community has dealt with many technical and other challenges to information sharing in the past, these challenges are poised to grow with the expansion of broadband cellular networks and associated data sharing platforms.

Given the relatively recent proliferation of data sharing platforms for public safety applications, it is not surprising that these challenges persist. However, since data exchange systems are not yet universal across the existing emergency communications ecosystem, different possibilities still exist for paths toward interoperable cross-agency real-time data exchange. The following sections describe some of the key considerations the public safety community (including first responders, technology developers, policymakers, and researchers) faces in creating a future of seamless sharing of real-time incident information. These challenges are divided into three broad categories: technical, economic, and governance. **None of these challenges exists in a vacuum; decisions made in one area will have ripple effects on the others, and none can be solved without simultaneously tackling the others.** In blunt terms, even the most useful technical solutions will fail to be adopted if agencies are unwilling or not permitted to share the information with the necessary entities or if they cannot afford the product.

3.1. Technical Challenges

While many agencies have begun adopting data sharing solutions, significant gaps exist between user needs and potential solutions in this rapidly evolving ecosystem. As the number of products expands and more agencies adopt data sharing technologies and services, the lack of interoperability for **data formats and schemas** and for **data access control** will inhibit public safety users from getting the maximum benefit from these technologies. Some solutions to these technical challenges exist; however, their adoption for public safety data sharing technologies has thus far been extremely limited.

3.1.1. Data Exchange Interoperability

The U.S. Department of Homeland Security (DHS) SAFECOM Interoperability Continuum [8] describes a spectrum of data exchange interoperability ranging from file swapping (minimum) to two-way standards-based data sharing (maximum; Fig. 4). If such standards adoption is not achieved, intermediate approaches (use of common applications or software interfaces to translate between systems) can provide many of the features of standardized systems, but with important limitations which are discussed in more detail in Sec. 4.1. In addition to these technical achievements, full operational interoperability requires shared governance structures, which facilitate cross-agency coordination in technology implementation as well as standard operating procedures, training, and regular usage.

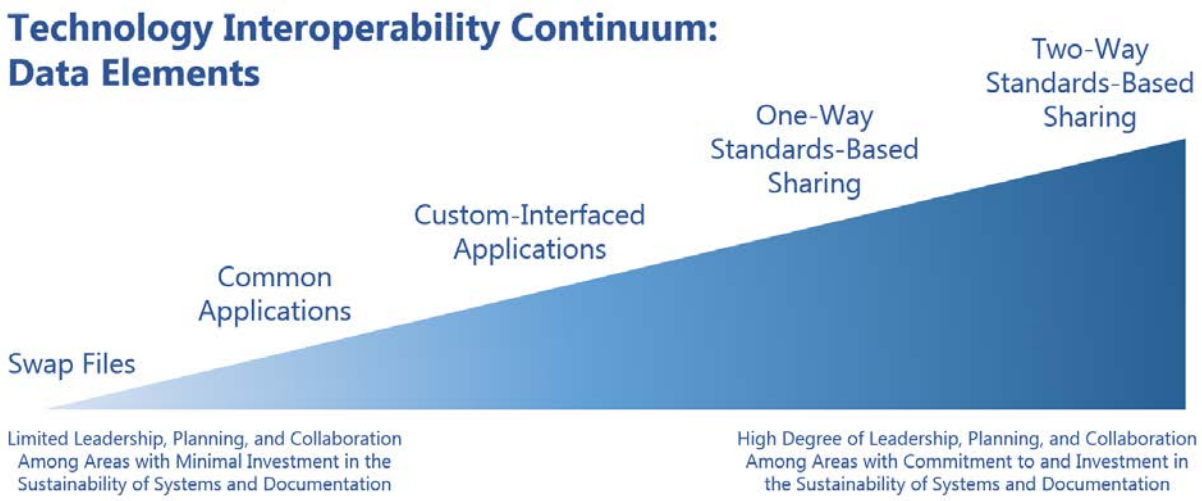


Fig. 4. Interoperability Continuum – Data Elements

The DHS Interoperability Continuum for communications technology data elements. In addition to technical interoperability, the Interoperability Continuum calls for coordinated development of communications governance, standard operating procedures, training, and usage.

The term "data exchange interoperability" is defined here as the ability for one software platform to receive and understand data generated by a different software platform. Data exchange interoperability requires each platform to follow a common set of definitions for the types of data it handles through the use of a standard defining the structure, content, and meaning of data being exchanged. Widely used meta-languages for data exchange standards include Extensible Markup Language (XML) and JavaScript Object Notation (JSON). XML and JSON are meta-languages in which a standard can be written, but they are not data exchange standards and therefore do not ensure that two systems exchanging data can understand and use the data being exchanged. For two applications to exchange mutually intelligible data, the data exchange standards they employ must not only be written in the same language, but they also need to use shared terms and definitions and follow the same relational structure (i.e., they must follow a shared schema). For example, a data exchange standard can define the data types (e.g., latitude-longitude geolocation, officer identity), data formats (e.g., WGS84 geodetic datum, alphanumeric character string), the ranges of allowable values, and other metadata properties. These definitions allow users of two different software platforms to send data to each other, and for the receiving platform to present the data to its users in the same way as data generated by its own platform. For practical purposes, a data exchange standard often includes a "data dictionary," providing descriptive text definitions of the data parameters included in the standard. As a simple example, if one agency uses an app that tracks the real-time locations of officers in the field, and they want to share their officers' locations with another agency using a different

location-tracking app, common data exchange formats for officer location and identity would allow both agencies to view the locations of all officers on their own respective apps.

Some data exchange standards for public safety information already exist or are in development by various SDOs. In this section, we highlight four data exchange standards developed specifically for public safety/emergency management applications (summarized in Table 1 and described in more detail in the following paragraphs).

Table 1. Notable public safety data exchange standards.

Standard Name	Description
Emergency Data Exchange Language (EDXL)	A suite of standards for emergency management data exchange, including Common Alerting Protocol, Distribution Element, Hospital Availability Exchange, Resource Messaging, Reference Information Model, Situation Reporting, and Tracking Emergency Patients [9].
National Information Exchange Model (NIEM)	A set of common, well-defined data elements for sharing information within and across domains including Agriculture; Biometrics; Chemical, Biological, Radiological and Nuclear (CBRN); Emergency Management; Human Services; Immigration; Infrastructure Protection; Intelligence; International Trade; Justice; Maritime; Military Operations; Screening; and Surface Transportation [10].
Emergency Incident Data Document (EIDD)	A set of specifications for exchanging data across IP-based Next Generation 911 (NG911) emergency communications systems [11].
NFPA 950	A framework for structured exchange of fire response-related data, including geospatial data, mutual aid and resource exchange, preparedness monitoring, and critical infrastructure. A future release of NFPA 950 will contain technical specifications [12].

The Emergency Data Exchange Language (EDXL) [13] is a suite of protocols for formatting information for public alerts, hospital availability and patient data, and other emergency communications. EDXL was developed as a component of the DHS Disaster Management eGov Initiative. The goal of the EDXL initiative is to facilitate emergency information sharing and data exchange across local, state, tribal, national, and nongovernmental organizations. It is managed and maintained by the Emergency Management Technical Committee of the international non-profit SDO OASIS. EDXL was originally designed as XML standards; however, its components are also being translated into JSON. As a suite of process-based standards, each EDXL component can be adapted to a variety of different

specific functions in a software implementation based on the needs of a particular use case (e.g., patient or responder tracking). Some components of EDXL are still under development, while others are complete and, in one case, in broad use. The most widely used EDXL component is the Common Alerting Protocol (CAP), which is used around the world for dissemination of alerts to the public and can also be used for sharing alerts privately. In the United States, FEMA provides IPAWS for the aggregation of all alerts (from local sources, the National Weather Service, the Environmental Protection Agency, etc.) then disseminates them to the affected communities via wireless emergency alerts. Other completed components of EDXL include the Distribution Element (a standard message distribution framework to facilitate the routing of any properly formatted emergency message), Hospital Availability Exchange (standard messages for communicating hospital status, services, and resources), Resource Messaging (standard messages for requesting and providing equipment and personnel), and Tracking of Emergency Patients (a messaging standard for exchange of emergency patient and tracking information). The Tracking of Emergency Patients standard was jointly developed with the SDO Health Level 7 International (HL7), which has developed many widely used data exchange standards for electronic health information. EDXL's Hospital Availability Exchange standard is now also a joint product of OASIS and HL7. We are not aware of any quantitative assessments of adoption; however, authors' personal discussions with individuals involved in EDXL's development and public safety technology developers suggest that adoption of components of EDXL other than CAP by public safety software developers has been limited.

The National Information Exchange Model (NIEM) [10] is a structured information sharing framework, first released in 2006, which developed as an extension of the Global Justice XML Data Model. The NIEM community is led by DHS, the U.S. Department of Justice, and the U.S. Department of Health and Human Services, together with a range of stakeholders from state, local, territorial, and tribal governments and the private sector. NIEM is composed of various domains ranging from emergency management to agriculture to transportation. NIEM is not a standard or set of standards, but rather a reference model made of XML schema documents known as Information Exchange Package Documentations, which contain structured and tagged data elements. Data elements are organized into two vocabularies: a core of data elements shared across all NIEM domains and community-specific vocabularies designed for each individual domain. The model leverages external standards, including EDXL components and standards developed by the Open Geospatial Consortium (OGC). NIEM is in the process of being adapted for JSON environments. A number of public safety and public safety-related entities use NIEM [14].

A related standard developed for the 911/dispatch community is the Emergency Incident Data Document (EIDD) [11]. This standard, developed through a collaboration between APCO and NENA, codifies definitions and formats for information to be shared among Public Safety Answering Points (PSAPs) within Next Generation 911 (NG911) systems, and could extend to sharing 911 call information with first responders. EIDD is also XML-based

and will likely be updated for JSON compatibility in the future. EIDD implementation into public safety software products has been limited, in part due to the need for the addition of an Incident Data Exchange functional element [15] as well as the incomplete implementation of IP-based NG911 networks across the country [16][4].

An incident data exchange standard for the fire service is under development by NFPA. The standard, NFPA 950 [12] (and its companion information sharing system implementation guide, NFPA 951 [17]), will include specifications for geospatial, text, image, audio, and video data exchange. An initial draft of the standard was released in 2015, and an update including technical specifications is in progress. The initial draft of NFPA 950 calls for compliance with NIEM. Additional public safety data exchange standards are listed in Appendix B.

Implementing data exchange standards supports three key public safety communication objectives:

- **Effectiveness:** Standards minimize confusion, miscommunication, and misinterpretation that can result from missing contextual information.
- **Efficiency:** Standards support wide-scale understanding and transmission of information by machines, which minimizes the need for repeated back-and-forth communications and facilitates scaling up information sharing systems.
- **Transparency:** Standards facilitate wide-scale analysis of data use, which can improve evaluations of technology implementation, privacy impacts, and data misuse.

While standards such as those described above have generally not yet been widely implemented in commercial public safety technologies, initiatives such as the DHS Next Generation First Responder Apex Program are engaging the technology developer community to develop data integration systems based on open standards, including EDXL [18]. The National Institute of Standards and Technology (NIST) Public Safety Communications Research (PSCR) Division is also building laboratory demonstrations of data sharing systems to understand the capabilities and interoperability of existing commercial products. Such implementations can provide a model for developers interested in building such solutions, and an example for practitioners to see how complementary solutions work together.

Despite the extensive efforts that have gone into developing the standards described above, many questions remain about their suitability for emerging real-time public safety data sharing applications. For instance:

[4] The most recent data available at the time of writing indicate that many states have little or none of their geographical area served by NG911 capable services (see data element 3.2.3.3 in Ref. [16]).

- How can the public safety community establish consensus on the most appropriate data exchange standard(s) for a particular data type?
- How can solution providers be encouraged to implement open data exchange standards in commercial products?

This document does not attempt to answer these questions definitively, but to highlight key issues which the public safety community should consider in collectively answering them. The issues explored here are not specific criticisms of the existing data exchange standards described above but may help explain the limited adoption of such standards to date.

Even if *existing* standards were adopted across all public safety data sharing technologies, they would not cover the full range of data types that first responders are interested in using. If appropriate data exchange standards for a given application either do not exist or are not implemented for any reason, an alternative solution is to develop custom-built interfaces between particular applications (i.e., "custom-interfaced applications" in the Interoperability Continuum, Fig. 4). Custom-built interfaces between non-interoperable CAD systems often have significant limitations due to the lack of control by the operating agency, high cost, interoperability disruptions following software updates, and lack of scalability due to the need for another interface in order to integrate with additional CAD systems [2].

3.1.2. Interoperability of Data Access Control

Lack of interoperability for data access privileges also presents an obstacle for cross-agency data sharing. **Here, interoperable data access control refers to the ability of a data sharing platform to detect, authenticate, and authorize *inter-agency users* in a way that requires minimal direct interaction with the user and administrator(s).** This capability requires data sharing systems to share definitions of incident roles (defined by an individual's rank, the function of a device, policies pertaining to specific data types, etc.) and associated data access privileges. At present, public safety agencies utilize a myriad of different ranks, titles, and internal policies for determining data access privileges for internally-produced data, and mapping one agency's roles/policies exactly onto those of another agency is problematic. Seamless real-time data sharing across agencies will require that this translation be built into data sharing systems.

An interoperable data access control mechanism would not only allow users to reuse a credential to access multiple data systems (i.e., "single sign-on") [19], but would be capable of dynamically evaluating the credentials of users who are previously unknown to the system. Such a system could add (or remove) users without requiring input from the users themselves. Once common authorization features, definitions, and protocols are established and implemented by all participating applications and users (i.e., they are "federated"), users are automatically permitted to access the appropriate components of the system based on the attributes of the user and data type or incident-specific requirements applied to the system. Such a system is scalable to a potentially infinite number of users and applications, as

individual profiles of users and data privileges do not need to be maintained in separate repositories for each application [20]. An interoperable data access system also does not require incident commanders or information technology (IT) managers to divert their attention to grant or deny access for new users, a critical feature for first responders who cannot afford to be distracted from their immediate tasks to manage their communications technology [21]. These principles have long been recognized as key features of a federated identity, credentialing, and access management (ICAM) solution for users of the National Public Safety Broadband Network (NPSBN) [22], also known as FirstNet[5].

Sensor-based alerts are a major potential public safety use case where well-defined data access controls will be critical. For example, body-worn sensors detecting movement, heart rate, or ambient oxygen concentration and temperature could detect that the wearer is potentially in distress [23]. When a sensor detects a threshold value, sending the appropriate alert to the appropriate recipient(s) requires the system to determine (1) who has permission to see the information, and (2) which users, devices, cloud services, etc., receive an alert about the information. Some users may have permission to view the information but do not have a critical need to access it immediately while other users may have both a critical need to access the information *and* to act on it immediately. These different types of users all require data access but they have different alert requirements, which may be extremely nuanced depending on the type of data and the incident circumstances. This document focuses on how technology can be used to address the issue of cross-agency data access in an interoperable manner, in order to carry out an agency's operational goals and policy restrictions. The issue of alerting prioritization warrants additional consideration beyond the scope of this report.

As data collection and distribution technologies become more sophisticated and ubiquitous in emergency incident response operations, information sharing procedures will require coordinated technical and policy frameworks in order for such technologies to be useful and compliant with applicable laws and agency policies. For example, if a sensor system detects a dangerous heart rhythm from a firefighter, it would not be ideal for the sensor data (which includes health information and PII) to be accessible to any user of the broadband network; it may also not be preferable for the data to only be accessible to an incident commander, if alerting other firefighters could allow for a faster rescue response.

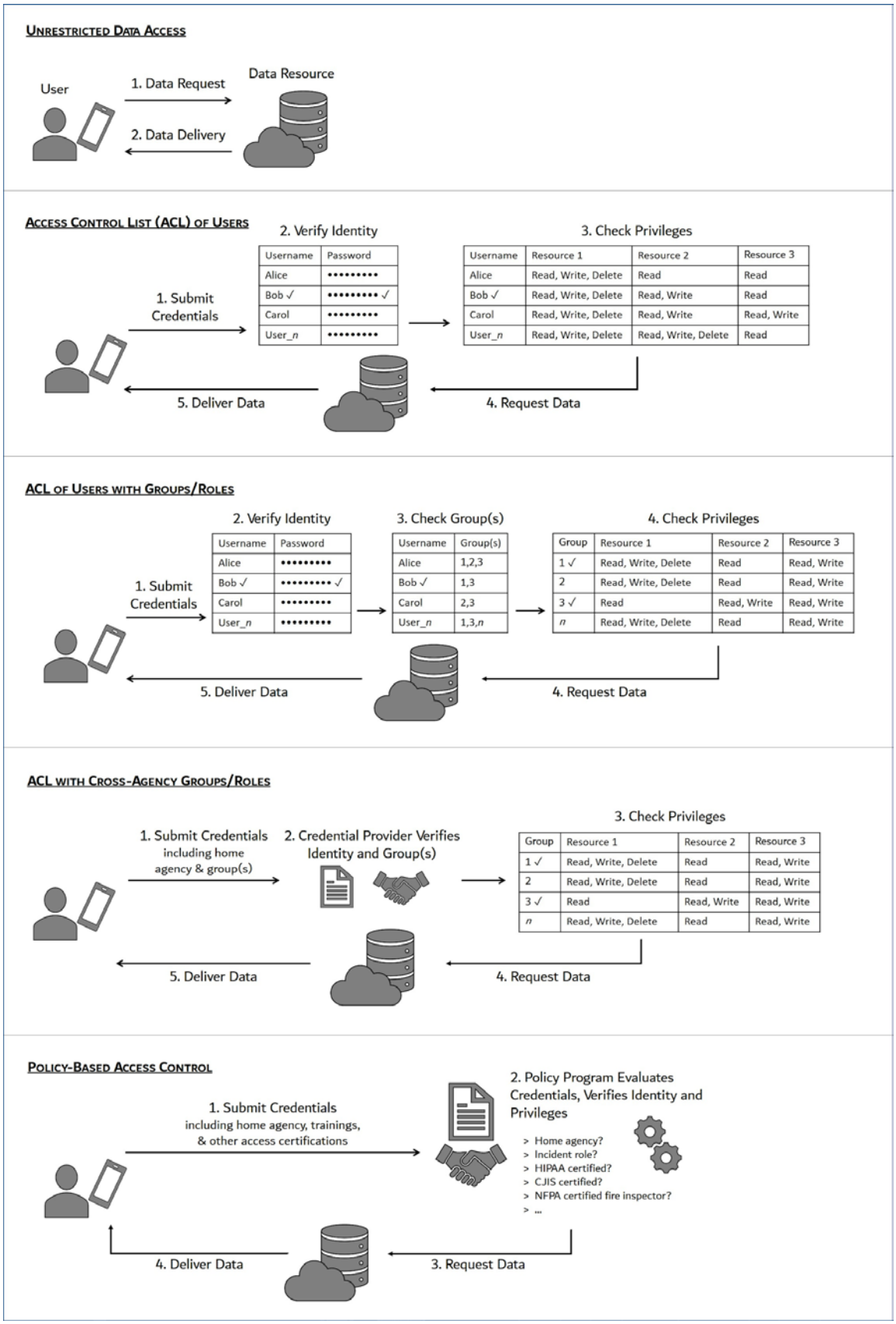
Policies supporting interoperable data access control should be implemented to ensure that information is only accessible to responders who are permitted to see it and alerts are sent to people/devices where it can be effectively utilized to accomplish mission objectives. Such policies, encoded in the architecture of access control and incident data collection and transmission, will be difficult to create. Different use cases and circumstances may require different policies, and the full range of possible contingencies will be difficult to

[5] https://www.firstnet.com.

envision in advance. It may not be possible—and likely is not desirable—to remove all ad hoc human decision-making from incident information sharing procedures. However, some software-enabled inter-agency data access policies will be necessary for advanced data sharing technologies to provide seamless and scalable solutions across a range of incident types and levels of complexity.

3.1.2.1. Approaches to data access control

In order to build trust between public safety users and new data sharing tools, and among public safety agencies, clearly defined data access policies, with sufficient granularity and nuance, will be critical. In the following section, we discuss various approaches to data access control, based on models developed in computer security research [24, 25], in the context of public safety data sharing applications. These approaches range from the simplest possible approach (no restrictions on who can access information) to a highly complex approach (policy-based access control), which would require extensive development and testing to be implemented in a public safety context (Fig. 5). Existing public safety data sharing applications generally fall in the middle, with access to a given platform permitted for a list of users possessing account credentials. Many public safety agencies utilize an enterprise access control system, which allows authenticated users to access certain components of the system according to privileges associated with the user's account. Another commonly used access control tool is a virtual private network, which creates a secure connection between a device and a private network, allowing system users to access private network content through a public Internet connection. For incidents requiring multi-agency response, secured electronic resources can be extended to new users by providing individuals with account credentials; however, this requires time and may not be suitable for resources with certain access restrictions. This spectrum of relatively simple to complex approaches is presented to demonstrate that there are alternative access control models available to those that are currently being used. The potential benefit for public safety operations of moving towards more advanced access control approaches warrants careful consideration by both practitioners and technology developers.



Username	Password
Alice	•••••••••
Bob ✓	••••••••• ✓
Carol	•••••••••
User_*n*	•••••••••

Username	Resource 1	Resource 2	Resource 3
Alice	Read, Write, Delete	Read	Read
Bob ✓	Read, Write, Delete	Read, Write	Read
Carol	Read, Write, Delete	Read, Write	Read, Write
User_*n*	Read, Write, Delete	Read, Write, Delete	Read

Username	Password
Alice	•••••••••
Bob ✓	••••••••• ✓
Carol	•••••••••
User_*n*	•••••••••

Username	Group(s)
Alice	1,2,3
Bob ✓	1,3
Carol	2,3
User_*n*	1,3,*n*

Group	Resource 1	Resource 2	Resource 3
1 ✓	Read, Write, Delete	Read	Read, Write
2	Read, Write, Delete	Read	Read, Write
3 ✓	Read	Read, Write	Read, Write
n	Read, Write, Delete	Read	Read, Write

Group	Resource 1	Resource 2	Resource 3
1 ✓	Read, Write, Delete	Read	Read, Write
2	Read, Write, Delete	Read	Read, Write
3 ✓	Read	Read, Write	Read, Write
n	Read, Write, Delete	Read	Read, Write

Fig. 5. Approaches to data access control

[see Fig. 5 on previous page] Conceptual visualizations of different approaches to controlling access to data. "Users" are visualized as humans, but they could also represent machines, such as Internet of Things devices communicating with other devices, databases, cloud servers, etc. Note that the number of components shown for each approach is not an indication of the level of complexity or difficulty in building a system using that model. See Sec. 3.1.2.1.(1-5) for details.

3.1.2.1.1. Unrestricted Data Access

An unrestricted data resource can be accessed by anyone who knows the location of the resource (e.g., through a weblink). Unrestricted systems include those which require users to register but does not require possession of any credentials (e.g., verification of their association with an agency). Unrestricted data access can also exist within a shared internal network, meaning that any user with a valid credential has full access to certain shared resources regardless of agency or rank or other role or credential (e.g., non-sensitive data such as weather information). Although data access is not restricted, users could be monitored. An unrestricted system is relatively simple to set up and administer and easy to use; however, it offers little or no security. It is unlikely that an unrestricted access system would allow users to add, edit, or delete data; such privileges would presumably call for more restrictive access control (as described in the following sections), which could exist as a separate component of a system with unrestricted *download* privileges for all users.

3.1.2.1.2. Access Control List (ACL) of Users

Using an Access Control List (ACL) of users, a system administrator maintains a list of authorized users, who may have specific privileges for viewing, adding, editing, and/or deleting data. In such a system, addition and deletion of users is manual. Users must log in to access each application, which can be done explicitly or through cached credentials. An "ACL of users" system is easy to understand and easy to use (especially if cached credentials are employed)[6]. The system is also simple to administer, provided the number of users and changes to the ACL are manageable. Administration becomes cumbersome and inefficient as the number of users and the frequency of updates to the ACL grow (which could be the result of both built-in technical limitations and resource/personnel constraints).

3.1.2.1.3. ACL with Groups or Roles

This approach, sometimes referred to as Role-Based Access Control (RBAC), builds on an "ACL of users" to define privileges (view, add, edit, and/or delete) for groups (e.g., "lieutenants")[7]. Groups are linked to another record of individual users (e.g., "John" is in the groups "lieutenants" and "station 1"). Access is performed in the same way as for "ACL of users," but the permissions associated with each user are based on permissions assigned to

[6] Cached credentials can carry a security risk because users may retain the ability to access a system even if the application cannot or does not verify with the credential provider that the credential is still valid.
[7] A well-known RBAC implementation, ARBAC97, specifies a notion of role hierarchies and a model for how role membership, role permissions, and role relationships are managed [26]. Other well-known RBAC implementations include Microsoft Active Directory [27, 28] and Oracle E-Business Suite [29].

their group(s). Like “ACL of users,” “ACL with groups/roles” has the advantages of a simple, straightforward model, so long as the number of users, groups, applications, and actions does not become too cumbersome. It has the additional benefit of not requiring administrators to assign individual access permissions to new users (or individually revoke them later), since they are automatically granted the permissions associated with their group(s). Ideally, group/role memberships would be assigned to each individual’s credential in a way that is mutually understandable across agencies, for example using the National Incident Management System (NIMS) National Qualification System [30]. In a public safety context, a system using “ACL with groups/roles” would need to be capable of interpreting privileges for individuals with multiple roles and dynamically adjusting privileges to accommodate temporary roles (e.g., current incident commander).

3.1.2.1.4. ACL with Cross-Agency Groups or Roles

Building further on the ACL model, this access control approach defines permissions associated with groups/roles that are shared among multiple agencies. **When a new user joins an incident led by another agency, the groups assigned by their home agency automatically grant them a particular level of access to information provided by any participating agency.** This would require cross-agency shared definitions of different incident roles. Designing such a system is technically similar to defining group access permissions for a single agency and would allow for seamless addition and removal of users in a complex multi-agency incident. The difficulty lies in bringing every participating agency into agreement about the various levels of access privileges for different data types, and rests on all participating agencies’ willingness to trust every other participating agency’s judgment about which individuals are assigned to which roles/groups. Additionally, every participating agency must agree on whether exceptions can be made to the permission rules, and, if so, they must trust that the other agencies will enforce exceptions appropriately. Finally, this approach requires a trustworthy, reliable method of verifying the identities of individuals from all participating agencies, that is, a credential provider. Every participating agency must also keep their group/role membership records up-to-date, which may require some coordination with the credential provider. It is worth noting that, for such a federated access control system to provide useful data to all participating agencies, the system would need to provide data in formats that can be ingested and interpreted by the various agencies’ own systems (databases, apps, incident dashboards, etc.), meaning that this level of access control federation warrants the implementation of data exchange standards.

3.1.2.1.5. Policy-Based Access Control

A policy-based access control approach moves beyond the need for an ACL. Under this approach, system administrators maintain a list of “rules” that specify what type of user can access what type of information. These rules are basically very small software programs,

which are run every time access is requested. The most common form of what we would call "Policy-Based Access Control" (PBAC) is Attribute-Based Access Control (ABAC) [31][8].

3.1.2.2. Attribute-Based Access Control

The basic model of an ABAC system is that each protected resource (i.e., file, service, etc.) has a set of known properties called attributes (e.g., owner, classification, sensitivity, purpose, type, etc.), and similarly each would-be user has a set of known attributes (including identity and roles, but also other characteristics of interest such as clearance levels, current assignment/tasking, completed trainings, certifications, etc.). Additionally, many ABAC systems allow other conditions about the world (such as time of day, physical location, overall threat level, user-/data-specific threat assessment, etc.) to be considered as well. In this model, administrators write rules that consider any combination of attributes to produce a ruling, for example[9]:

```
if user.identity is resource.owner then ALLOW,
```

or

```
if user.identity is firefighter and resource.type is
"building plans" and context.current_mutual_aid_incident
is TRUE then ALLOW and AUDIT
```

In this example, the owner of the building plan documents would always be allowed to access them; any firefighter responding to the current mutual aid incident would also be allowed access, and their use of the resource would be monitored. **The power of such systems is that they are highly *expressive,* meaning that the administrator can define rules which capture much more subtlety of what is or is not allowed for a particular user, relative to RBAC or ACLs. The flip side of expressiveness is *complexity*: An individual rule can be complex on its own (e.g., by containing multiple conditions and dependencies on other rules), and multiple rules can apply to the same operation.**

Examples of ABAC policy languages include eXtensible Access Control Markup Language (XACML) [32], Next Generation Access Control (NGAC) [33], Binder [34], JSON Access Control Policy Language [35], SecurOntology [36], PolicyMaker [37], KeyNote [38], RT [39], and SDSI [40]. Some of these systems are mature but some are experimental (e.g., to

[8] Attribute-Based Access Control is generally different from Attribute-Based Encryption (ABE). The basic model of ABE is that data are encrypted in such a way that the cryptography itself enforces a desired ABAC policy: users' keys are generated in a way that in effect encodes their attributes, and protected data are encrypted in a way that is decodable only by keys corresponding to the desired combination of attributes. Since the policies and attributes are essentially "baked in" when data are encrypted and keys are issued, context information and time-varying policies (or attributes) are not supported with ABE.

[9] This is not valid code in any real policy language. Unfortunately, most are more cumbersome, and more background is necessary to read them. In this simplified example, "ALLOW" would permit the user to access the resource, and "AUDIT" would create a log of the user's actions upon that resource.

our knowledge, only XACML and NGAC have been approved by SDOs, and only XACML has been implemented commercially).

3.1.2.3. Trust Management

ABAC invites the question of "where do the attributes come from?" Resources or objects can have their attributes specified either automatically by the systems that create/manage them, or manually by their owners. But users' attributes must be conveyed to the access control engine in a trustworthy way from a trusted source, for example using a digital signature with public key cryptography. In the case of cross-agency authorization, we have the same problem as for cross-agency roles: even if the federated ICAM process works perfectly and is absolutely secure, we may not be sure how much to really trust the credential issuer.

The basic model of Trust Management is to be able to specify formal policies for automated reasoning around who the system believes about what[10]. Such systems are extremely powerful: consider the extreme case where there has been a major disaster and communications have been badly damaged. Personnel from two agencies are responding to the same events, but they have never had the opportunity to set up any kind of mutual awareness in their computers. Under a Trust Management scheme, Agency A could specify, for instance[11]:

```
Trust NCIC to say an entity is a law enforcement agency;

Any law enforcement agency is a public safety agency;

Trust any public safety agency to identify their key staff;

Trust any person who is key staff for any public safety agency
to assert that any other person works for the same public
safety agency (and to assert their rank, function, etc.).
```

According to these rules, if Agency B is an accredited agency according to the Federal Bureau of Investigation's National Crime Information Center (NCIC), Agency A will trust Agency B's assertions about the identities, ranks, functions, and other qualities of Agency B's staff. Likewise, if Agency A needed to work with someone from Agency B, despite having never interacted previously (and having no ability to communicate with either agency's servers), Agency A's equipment could likely determine that credentials from Agency B are trustworthy (according to the above rules) and grant access to Agency B personnel.

---

[10] Note that this is still in the context of computerized access control, not real human interactions, so the point is to, in a federated and automated way, determine whether or not to trust an electronic credential issued by some party *x* asserting some supposed fact *y*; and if the system does not already automatically trust the credential, determine whether there is some additional information that would cause it to do so.

[11] These rules are for illustrative purposes only and do not constitute actual instructions in any specific computer language, or recommendations for encoded policies.

The downside of that kind of capability is complexity: To deal with the variability of real trust relationships, Trust Management decision processes generally need to be fully-capable automated logical reasoning systems, which are both technically difficult to design and may not always be able to find a solution quickly [41, 42]. Finally, from a practitioner perspective, the operation of policy-based access controls is generally opaque to the individual user.

Without the need to manage an ACL, a well designed and implemented PBAC system could be implemented for a potentially infinite number of users and applications. Policy-based access control could be carried out in a process of iterative computational negotiations, where a user's request for access to a resource is contingent on a series of verification steps to confirm their identity, role, and other features. The primary difficulties in establishing policy-based access control lie in (1) establishing consensus on the meaning of credentials from different credential providers and (2) choosing appropriate policy languages and writing software programs that consistently and correctly execute the actual access control policies. Making decisions about access control approaches across multiple agencies calls for a high degree of trust between the participants. Any existing working relationships between public safety agencies can be used as a foundation for data sharing and access control federation.

One organizational credentialing and identity federation framework that has gained popularity in the first responder community is the Trustmark Framework [43–46]. The Trustmark Framework operates by issuing XML or JSON credentials to organizations based on their conformance to policy agreements established for particular information sharing purposes. It is meant to be extremely granular (and therefore modular), and to allow agencies to develop trust relationships based on their specific requirements without the need for formal information sharing agreements between individual agencies. The Trustmark Framework improves the trust aspect of the Public Key Infrastructure model by broadening the scope of attributes to be verified. The Trustmark Framework relies on certified Trustmark Providers that assess entities and issue trustmarks to those entities based on some evidence that the entity (called a Trustmark Recipient) conforms to the relevant policies as captured in one or more modular Trustmark Definitions. In practice, agencies would require their information sharing partners to conform to Trust Interoperability Profiles, which are collections of Trustmark Definitions that represent policies such as NIST SP 800-53 [47], the Federal Bureau of Investigation's Criminal Justice Information Services (CJIS) Policy [48], or the Health Insurance Portability and Accountability Act (HIPAA) [49].

A final risk with all of the access control approaches described above is the assumption that authentication and authorization can be carried out over the Internet. Many public safety use cases involve degraded network environments, where constant internet connectivity cannot be guaranteed or only a local deployed network is available. It is therefore worth considering bridging a chosen authentication approach with more flexible methods that do not rely on a

backhaul connection. For example, a system could have a process for allowing a certain number and/or type of authenticated users to collectively authenticate a new user.

Technical Challenges: Key Takeaways.

- Existing data exchange standards do not cover the full scope of data types used by public safety and have not been widely implemented in commercial solutions.
- Inter-agency data sharing interoperability requires a federated ICAM solution that allows agencies to add and change first responder data access privileges in a rapid and secure manner.
- Public safety agencies should follow and participate in efforts to develop standards and ICAM guidance, and implement the guidance from entities like the SAFECOM ICAM Working Group as it emerges.

3.2. Economic Challenges

Making disparate real-time data sharing technologies interoperable has clear benefits for users; however, it also creates direct and indirect costs, which may be reflected in product/service prices and personnel hours. The benefits of data interoperability contend with the realities faced by technology developers (whether in private industry, government, non-profits, or academia), who must deliver products to their customers through a sustainable development process. As public safety communication systems continue to incorporate the sharing of more diverse data types, a careful consideration of the implications for agency budgets will be critical. It is important for both technology users and developers to recognize the trade-offs they each face when considering possible solutions to data interoperability, so that public safety agencies and vendors can collaboratively determine the best approach for a given technology or service.

For the purchasing public safety jurisdiction, the economic analysis of whether to select an interoperable or non-interoperable data product is essentially a cost-benefit analysis between any financial cost of implementing and maintaining a standard-compliant system (or translator/interface between systems) and the efficiency savings achieved through standardization. The resources required to establish and maintain a standard or interface (and associated labor from staff with the necessary expertise) will vary considerably from one application to the next, and therefore must be assessed on a case-by-case basis and should be re-evaluated throughout the development and implementation process. As the standard may evolve over time and the product may change, some resources will need to be devoted to maintaining the standard or interface throughout the lifetime of the product.

The benefits of standardization may be more difficult to quantify in advance; however, they are potentially significant. Standardization offers economies of scale by making it relatively easy to add new use cases (e.g., integrating data streams from multiple different apps) and

collaborators (e.g., collaborating with a new agency or external stakeholder), which could lead to significant **operational efficiencies**. Standardization can also encourage **market competition** by lowering the barrier to entry for companies without an established presence in public safety. Additionally, standardization can make all data sharing platforms more useful by increasing the **number of data sources that are available** to any individual platform and user, which is likely to increase the number of applications and users (i.e., a network effect or positive feedback loop).

Agencies can assess the potential for improved operational efficiencies by discussing potential use cases for integrated data sharing and visualization systems within their agency and with their stakeholders. When negotiating data interoperability solutions with vendors, agencies should inquire how implementation and maintenance costs will affect the cost of using the product over the course of the full technology life cycle. Implementing new technologies is of course associated with a direct cost of acquiring new devices or, increasingly, web-based services (such as a mobile application subscription or cloud data storage). In the case of web-based services, standards conformance could impact the cost to users beyond just the initial investment due to the subscription model of many web-based services.

New data sharing devices and platforms also require new **training** for responders, communications center personnel, and agency leadership. So long as new communication technologies do not supplant legacy technologies, their adoption may mean more time, and therefore money, devoted to activities other than responding to emergencies. However, to the extent that the technologies increase communications efficiency and effectiveness (e.g., by diverting a portion of LMR communications to group text messages), the investment of time and resources may actually increase the time and resources responders can devote to their non-communication tasks. Furthermore, training for interoperable systems could be more efficient, due to the relative cognitive complexity required to use them, than for a system comprised of non-interoperable tools that perform the same functions.

Managing digital communication platforms such as biometric sensors, video streams, and analytics systems requires **technical support and management** of a different kind than what is necessary for LMR systems. Lack of data interoperability threatens to make the work of agency data managers even more challenging, as each system an agency acquires has a different technical architecture and user interface, requiring more training for both IT administrators and users in the field. Non-interoperable systems lend themselves to **cost redundancies**, as each system operates on its own equipment, leading to higher costs for device acquisition and maintenance than would be necessary if a system could be assembled *à la carte* and all data could be synthesized in a single platform. As the use of digital tools expands, agencies will face the decision of whether and how to support additional staff or contracted technical support to ensure the security and functionality of the tools, and how these resource needs are impacted by data sharing interoperability (or lack thereof). **The**

economic consequences of siloed systems will encourage agencies to choose the set of products that they can afford and manage, which may constitute fewer capabilities than they would be able to adopt if the available technologies were modular and interoperable.

Finally, as with any new technology, the technology developers and vendors have somewhat different objectives from those of public safety users. Developers want to ensure that they maintain an advantage over their competitors, which in emerging technology sectors can mean limiting cross-platform data sharing interoperability to promote **customer lock-in**. Users share this objective to the extent that they need vendors operating under a sustainable business model; a vendor that goes out of business cannot provide feature upgrades, software updates, or security patches. However, the inability to share data across platforms requires public safety agencies to commit to a single provider for each data sharing application and prevents them from integrating data streams from various platforms in the manner that best suits their needs [50]. For example, a fire department that wishes to implement a variety of body-worn and environmental sensors may find that the collection of products that best meets their needs requires a separate, proprietary data integration hub and graphical interface for each product. The department now faces the choice between a system that requires their firefighters to wear an excessive number of devices and their commanders to view data streams on separate display monitors, or an all-in-one system from a different vendor that doesn't provide the preferred functionalities of the custom-built solution. Furthermore, **vendors may consider the data and analytics their platforms provide to be proprietary**, meaning users will have limited access to the data if they wish to use it for purposes beyond the immediate function of the platform itself. Vendors may also wish to use the agency's data for business purposes, such as research and development of new products. Because incident data holds value for developers and vendors in the form of advanced features and possibly access by third parties, vendors may choose to allow agencies to access and retain data or integrate it with other platforms only at a **higher subscription cost** (a practice used by some CAD providers). These distinct interests, which are sometimes at odds, present a challenge to public safety agencies hoping to adopt novel data sharing technologies at an affordable price.

Ideally, public safety users and technology developers would be able to reach a consensus on the appropriate **balance between standardized data sharing functionality and product-specific innovations**. For example, fire departments may determine that being able to share the locations of specific resources is operationally critical to any location-based incident data sharing. Technology providers would then implement a standard defining the meaning and data formats for identities of fire trucks, department headquarters, and personnel, and their associated geospatial coordinates. Any features beyond these resource location data could be non-standardized, allowing technology developers to compete for customers. As a particular technology becomes more mature, the number of features considered fundamental, and therefore expected by users to be standardized, may grow. Finding this balance may be

difficult at first, but it will help ensure that both public safety users and vendors can benefit from standardization.

Economic Challenges: Key Takeaways.

- Compared to proprietary end-to-end solutions, interoperable data sharing solutions would provide reduced equipment acquisition and maintenance costs, reduced training needs, and more flexibility in choosing the suite of capabilities that best meet their needs, regardless of vendor.
- Standardized data sharing tools present a risk to vendors through reduced customer lock-in. However, vendors, especially less established entities, can benefit from lower barriers to market entry and a broader potential customer base.
- Vendors and agencies would benefit from community consensus on baseline data sharing functionalities requiring standardization; additional functionalities constitute opportunities for innovation.

3.3. Governance Challenges

At present, public safety agencies implementing data sharing technologies qualify as early adopters. They are motivated by the benefit these technologies could provide to their mission alongside legacy emergency communications systems, and they are exploring how best to integrate them into their regular operations. In contrast to established technologies such as LMR, consensus-based standard operating procedures or guidelines, implementation guidance protocols, or frameworks for cooperating with partner agencies developed for data sharing technologies are very limited. Without such support, many agencies will likely find it difficult to plan and implement effective data sharing initiatives, and to sustain their initiatives throughout changes in leadership [51].

Existing groups and structures can serve an important role in helping local agencies coordinate interoperability initiatives at larger geographic scales than their usual partners for daily operations. Each state internally develops a State Interoperability Executive Committee (SIEC) [52] or Statewide Interoperability Governing Body (SIGB), which considers interoperability issues and makes recommendations to state authorities regarding policies and procedures. At the national level, the DHS SAFECOM program supports a Statewide Interoperability Coordinator (SWIC) for each state and territory. The SWICs lead the implementation and updating of a state's Statewide Communication Interoperability Plan and participate in the National Council of SWICs (NCSWIC). For interoperability issues related to the deployment and use of the FirstNet network, agencies can engage their state/territory Single Point of Contact (SPOC) to provide their perspective and track developments. Each state also has an administrator for statewide 911 issues, who coordinates across states through the National Association of State 911 Administrators (NASNA). **Engaging with these state-level bodies therefore allows agencies to learn about and influence**

interoperability programs across their state and the nation. If particular states or regions wish to embark on developing governance structures and policies for particular data sharing systems or use cases, these bodies could support their efforts by connecting agency leaders to one another and disseminating their guidance and lessons learned to the nationwide public safety community.

Strong interest in particular technologies has inspired various organizations to develop specific guidance for use in public safety applications. In the case of unmanned aerial systems (UAS), the Federal Aviation Administration provides resources on federal regulations affecting UAS use in public safety [53], while the National Conference of State Legislatures tracks developments in state UAS laws [54][12]. The National Public Safety Telecommunications Council [55], the American National Standards Institute UAS Standardization Collaborative [56], and the National Council on Public Safety UAS [57] have developed resources and recommendations for agencies considering implementing a UAS program, including considerations for data sharing and management.

However, for many emerging data sharing technologies, agencies implementing solutions today are largely left to determine best practices on their own. Many federal and state privacy statutes restrict public disclosures of personal information, but such laws generally do not address the exchange of personal or incident-sensitive information among public safety agencies or define how such data are to be managed within an agency. Because the variety of potential data elements that could be shared among public safety agencies is vast and includes information ranging from mundane (e.g., traffic camera footage) to extremely sensitive (e.g., images of criminal suspects), determining rules for data access can become extremely complex. Agencies may be concerned that, even if they have implemented strong data security procedures, they cannot control how their data are protected once they are shared with other agencies. Agencies may wish to prioritize caution when implementing data sharing capabilities for sensitive data types to minimize unanticipated problems that could result from sharing information with unnecessary or inappropriate individuals [58]. A useful approach to adopt when data security is a concern is to establish logging and auditing procedures, enabling data use patterns to be analyzed and possible incidents of misuse to be appropriately investigated.

Agencies can also develop their own policies and best practices. The U.S. National Telecommunications and Information Administration has recognized this need by encouraging states to pursue data sharing policy development activities in their FirstNet implementation grant proposals [59]. Governance structures could include a combination of formal agency policies and inter-agency memoranda of understanding, as well as voluntary guidance and reference documents, and could leverage pre-existing mutual aid agreements. Such governance structures will need to be flexible enough to evolve as technologies change

[12] State laws generally concern privacy protection and some specifically address UAS use by law enforcement agencies, for example requiring the collection of flight records and warrants for surveillance or searches.

and agencies gain more experience sharing data across jurisdictional and disciplinary boundaries. For example, the rapid expansion of law enforcement use of body-worn cameras has demonstrated the need for carefully articulated video data management policies. A recent report from the DHS Video Quality in Public Safety group outlines key features that public safety video data policies should address [60]. **Building on these recommendations, we propose the following elements that public safety agencies should address in their data sharing policies:**

- *Data Definitions:* What data are collected? Are they shared in real time, with time delay, or only following an incident? The following considerations may be different for different data types.
- *Data Management:* Who is responsible for maintaining different data elements during an incident?
- *Data Ownership:* Who owns the data generated by an agency (the agency itself, or a third party)? How is ownership affected by sharing data with another agency?
- *Data Access:* Who is allowed to access, download, write, change, or delete the data and how is that controlled? In the event of unauthorized data access, what procedures are required for informing affected agencies or other parties and containing the breach?
- *Data Security Practices:* How are data protected from unauthorized use (copying, modification, deletion, etc.)? In the event of unauthorized data use, what procedures are required for informing affected agencies or other parties and containing the breach?
- *Data Integration:* How are incident data integrated into other agency data systems (dispatch/CAD data, accounting data, Records Management System data, forensic data, evidentiary data, etc.)? Are specific data exchange standards employed to achieve this?
- *Data Retention:* How long are data retained (minimum and maximum time periods)? If copies are made of the data, how are they managed after an incident, or after the retention period has ended?
- *Data Redaction:* How is sensitive data or PII defined, flagged, and removed from records for internal retention and public records requests?
- *Data Policy Consistency:* How will differences in the above policies be resolved?

Additional details and considerations for these elements are explored in more detail in the use case in Appendix A.1. As more agencies build a foundation of experience and documentation, later-adopting agencies can leverage these resources and accelerate their own governance implementation. Examples of data sharing frameworks which could be adapted

to public safety operations are discussed in more detail in Sec. 4.3. **For agreements between a small number of agencies to be scalable, it would be ideal for the public safety community to create a body analogous to the Uniform Law Commission[13] to draft template agreements which could be easily adapted by specific agencies.** The use case shown in Appendix A.1 demonstrates the complexity of designing an agreement from scratch that addresses all the above features.

Governance Challenges: Key Takeaways.

- Data sharing governance structures are critical for establishing security requirements and meeting privacy and transparency/accountability laws and policies.
- Public safety agencies can build data sharing governance bodies by working with their existing mutual aid partners as well as state bodies including their SIEC, SPOC, SWIC, and statewide 911 coordinator, and federal bodies including SAFECOM, NCSWIC, and NASNA.
- Governance guidance on public safety UAS programs has been developed by NPSTC, the Federal Aviation Administration, the National Council on Public Safety UAS, and the American National Standards Institute.
- Data sharing policies should articulate the expectations and responsibilities of participating agencies for all aspects and stages of data sharing.

4. Charting a path towards interoperable real-time public safety data sharing

Given the speed with which new data sharing communication capabilities are becoming available, many agencies are choosing not to wait for formal guidelines or widely accepted best practices before implementing new technologies. This section describes steps agencies can take to build their internal capacity for real-time data sharing solutions, while coordinating with the larger public safety community to build a foundation of shared standards, policies, and procedures that can eventually facilitate secure, flexible, and fully interoperable data sharing across the emergency communication ecosystem.

4.1. The Risks of "Band-Aid" Solutions

Given the current lack of standardization for data elements within public safety applications, adopting common applications is the only practical approach for agencies wishing to ensure data exchange interoperability for all users. However, common applications can only be

[13] The Uniform Law Commission supports state legislatures in the United States by researching and drafting non-partisan laws that can be used as templates.

considered a partial, temporary solution to the challenge of data interoperability, as is evident from its low position on the Interoperability Continuum (Fig. 4). As an interoperability "solution," common apps represent significant risks (Fig. 6) and, by delaying action on the fundamental challenges, may push true interoperability solutions into the more distant future.

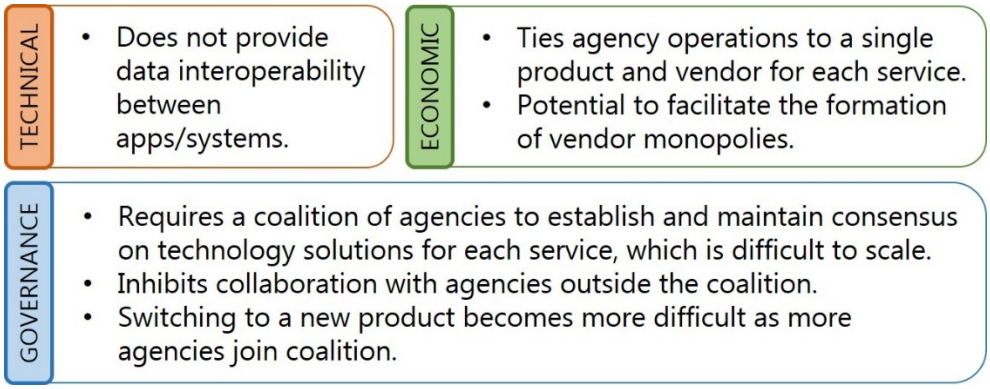


Fig. 6. Risks of common applications

Pursuing common applications as an interoperability solution carries significant risks without providing functional interoperability beyond each particular app.

For a single agency or jurisdiction with a single point of purchasing authority, acquiring common applications is relatively straightforward. Provided software updates and agency customizations do not disrupt interoperability between users, this approach makes it possible for all users of a particular application to share data with any other users of that application. An application may still employ access restrictions, such as by registering individual users to particular groups (e.g., Agency A). A governance body, composed of representatives of all participating agencies, could lead the evaluation and selection of technologies for the group and establish procedures to ensure that each application is controlled and paid for equitably. The body could also adjudicate disagreements between participating agencies related to the use of common apps. To ensure that decisions made by the body are implemented, these representatives would need to exert significant influence over their agency's purchasing decisions.

Cross-agency coordination is required to extend the data sharing capabilities of a single application to users from other agencies. Despite the obvious challenge of reaching consensus among multiple agencies, such a coordinated process may provide agencies with leverage when negotiating features, services, and prices with vendors, by creating a larger number of users than an agency acting alone represents. If common applications are not adopted in advance of an incident, they can be used ad hoc by encouraging other agencies to download the app during the incident, or by providing responding units with pre-configured devices, similar to an equipment cache. However, unlike swapping radios, adopting mobile applications on the fly may be more difficult and present unanticipated security risks for agencies that do not have the training and experience with a particular application [5].

More serious challenges may arise as agencies look to grow the group of coordinating agencies over time. A new agency considering joining the group may be able to influence future application decisions, but the applications already adopted by the founding group members may be non-negotiable. New agencies may therefore be reluctant to join if they do not fully support the decisions the group has already made (especially if their own agency has adopted different applications with similar capabilities) or if they believe that their position within the group is given less weight than that of founding member agencies. Even if these tensions do not exist, each additional agency participating in application adoption decisions will increase the complexity, and possibly decrease the level of consensus, of each decision. These challenges are worth considering when agencies weigh which partners to involve at the outset of a cross-agency collaboration and how they envision the collaboration growing over time.

In addition to the governance challenges of coordinating acquisition across every participating agency, common applications not fully compliant with open standards inherently lock-in an agency to the product's solution provider. The degree of this dependence on the vendor increases as additional agencies join the initiative. If an agency uses a product that generates data in a proprietary format, they may not be able to use the data for analytics outside that product's ecosystem. Choosing to switch to a different product or being forced to switch if the company goes out of business may prove very difficult and disruptive for the agencies. Furthermore, common applications without standardized data do not allow agencies to integrate data streams from the variety of products that they prefer; to avoid separate interfaces for each product, they will still have to buy a package of products from a single vendor.

As a long-term solution, common applications can lead to two possible outcomes: either every agency that wishes to work together adopts the same applications, or different consortia of agencies using different collections of "common" applications develop in siloes. In the first outcome, the vendors of the "winning" applications enjoy a monopoly for each particular solution, making agencies highly vulnerable to the decisions and the success or failure of each vendor. In the second outcome, the more successful each agency consortium is at expanding its membership, the greater the barrier to collaborating across consortia. The public safety community therefore deserves a more sustainable approach to data sharing interoperability than common applications can offer.

The Risks of "Band-Aid" Solutions: Key Takeaways.

- Common applications provide interoperability for users of a given app, but not for responders using other apps.
- Governance of common applications solutions is difficult to scale.
- Common applications encourage vendor monopolies and agency lock-in.

4.2. Specify Interoperability Requirements in Requests for Proposals (RFPs)

Funding bodies that support public safety agency technology acquisitions can support data exchange interoperability by recommending or requiring that RFPs require conformance or compliance with particular standards. This approach is already being taken in some cases, such as the recommendation to require conformance with EDXL in grant guidance from the SAFECOM program [61]. Similarly, the most recent National 911 Program procurement guidance for NG911 systems states that vendors should adhere to standards [62], though it does not specify particular data exchange standards such as EIDD that should be required. It is noteworthy that neither of these examples recommends that conformance with data exchange standards be an absolute requirement for vendors. Standard-conformant products are simply not available for every data sharing application and, given the current state of standards implementation, setting unrealistic or irrelevant standards requirements can make acquisitions unnecessarily costly for agencies [63]. To facilitate RFP and contract language that meets data exchange interoperability expectations, agencies and technology developers would benefit greatly from guidance documentation on recommended standards for emergency incident data, similar to the Interoperability Standards Advisory produced by the Office of the National Coordinator for Health Information Technology [64].

Whether or not agencies are aware of data exchange standards to which their desired solutions could conform, RFPs can articulate specific metrics of interoperability they require. For example, if an agency regularly participates in mutual aid activities with a neighboring department that has adopted a particular vehicle location tracking application, their RFP for vehicle location tracking solutions could specify that the vendor demonstrate that their solution can exchange location information with the neighboring department's application. The RFP could also stipulate whether or not the agency is willing to pay more for such a solution based on either non-proprietary data exchange standards or a custom-built interface between the two applications (see the discussion on custom-built interfaces in Sec. 3.1).

Finally, RFPs requiring conformance with data exchange standards create a need for conformance testing tools that agencies can use to vet products. Whether a tool is used by an agency to test the product before making a purchase or the vendor uses a tool to label their product, having a testing tool would simplify the procurement process for agencies and increase confidence in products that assert standard conformance. Such tools should be developed independently of commercial vendors with input from public safety technology users to ensure they demonstrate interoperability meeting the operational expectations of agencies, rather than interoperability as defined by the vendors.

These examples demonstrate that funding bodies are aware of their role in leading the public safety community towards adopting standards for data exchange interoperability. **The challenge lies in achieving consensus across the public safety community about which standards should be adopted and developing the collective commitment to hold vendors**

to these requirements (through testing and certification, where possible). Wherever such consensus exists, requiring data exchange standard conformance can provide an opportunity for the public safety community to collectively speak for interoperable data sharing solutions.

Specify Interoperability Requirements in RFPs: Key Takeaways.

- RFPs should specify operational interoperability requirements for data sharing technologies whether or not relevant data exchange standards exist.
- To specify interoperability requirements in RFPs, agencies would benefit from detailed, comprehensive interoperability guidance like that developed by the Office of the National Coordinator for Health IT.
- Conformance testing tools are needed to support agencies which specify interoperability requirements in RFPs and contracts.

4.3. Develop Data Sharing Policies by Building on Existing Frameworks

As data collection and sharing technologies become increasingly entrenched in modern life, fields as diverse as consumer products, healthcare, education, utilities, and public safety communication are all grappling with the technical, financial, and governance challenges of securely managing constantly growing datasets.

The Next Generation 911 Interstate Playbook [65] is a valuable resource upon which collaborating public safety agencies can build their data sharing efforts. Chapter 1 of the playbook summarizes the governance and financial considerations and mitigation strategies used by state 911 agencies working towards a cross-state integrated NG911 system, which include many of the issues presented in this report. The sample Memorandum of Understanding (MOU) language in the Playbook's Appendix 3 could provide a starting point for agencies drafting their own inter-agency or inter-jurisdiction data sharing policies.

Public safety agencies can also develop data sharing agreements using the guidance of the Standards Coordinating Council's Information Sharing and Safeguarding Playbook [66]. This resource describes the variety of components that planning, executing, and evaluating an information sharing initiative can include, including evaluating relevant standards and developing a data management policy. Each component includes specific questions agencies should ask in evaluating the task, and steps they can take to accomplish it, with an eye to all three categories of challenges identified in this document. Importantly, the final component of the playbook, "Make it scalable and sustainable," recognizes the importance of building a data sharing framework that can grow and adapt to changing circumstances and new information, and that can endure the vagaries of budgeting decisions. If this process is carried out as a collaboration between two or more agencies, it has the potential to lead to a pilot program demonstrating an actual implementation of an interoperable cross-agency data sharing solution.

Closely related to public safety data sharing use cases are government initiatives for "open data," [14] and "smart city" systems. Like public safety data sharing, these initiatives require both greater interoperability of datasets created by disparate entities and carefully crafted policy frameworks that protect data integrity and privacy while promoting data utility, enhancing transparency, and facilitating public accountability [67, 68]. Many cities in the U.S. have embarked on open data programs, for example Chicago, IL[15]; Washington, D.C.[16]; and Columbus, OH[17]. Although these programs are targeted at providing public agency data to the public rather than exchanging data among public safety agencies, they share many relevant objectives, features, and challenges. **If an agency serves a jurisdiction developing a smart city or open data program, public safety agencies can engage with leaders of these initiatives to leverage the principles, specifications, and governance structures for their own inter-agency data sharing plans.** This could include strategizing together with other government agencies, re-using RFP language, and sharing infrastructure and technical resources. Local collaboration could also be extended to larger areas through regional governance structures[18].

Data privacy is a major concern for open government data, as many public agency datasets contain PII, or data that could potentially be linked to re-identify individuals or subpopulations. Robust open data policies go into detail about the types of data being published, the steps taken to protect the privacy of sensitive data, and the measures in place to ensure that the objectives of the policy are being achieved [69]. An open data portal should be easy to use and maintain, leverage metadata to make data discoverable, and link information across data sources [70]. For example, the privacy policy for the Chicago Array of Things states that sensitive data will be protected both through cybersecurity measures (encryption) and redaction procedures (e.g., restricting the publication of surveillance camera footage to still images).

One framework which could be adapted to public safety data sharing initiatives is the privacy risk assessment model developed by the Future of Privacy Forum in their audit of the City of Seattle's open data portal [71]. The components of this model include identifying sensitive data, quantitatively comparing the benefits and risks of releasing the data, evaluating options for mitigating re-identification risks, and ultimately determining the most appropriate method for releasing (or not releasing) the data. In the context of public safety agencies or first responders sharing real-time incident data among each other, privacy risks result primarily

[14] "Open data" is defined as data which are "free for anyone to use, re-use and re-distribute" [67].

[15] Chicago's Array of Things project integrates a network of sensors collecting environmental pollution data, video imagery, seismic activity, and other information, which are available to the public.

[16] The Open Data DC platform provides public access to datasets of infrastructure, public safety, aerial imagery, and other city features.

[17] Columbus maintains the City of Columbus GIS Open Data Portal.

[18] For example, regional political bodies such as the Metropolitan Washington Council of Governments, or regional smart cities initiatives such as the Colorado Smart Cities Alliance.

from the possibility that unauthorized entities may obtain access to sensitive data (i.e., inadequate cybersecurity protection), as opposed to the risks of re-identifying individuals from linked data. However, if any incident data are stored on devices or servers beyond the length of a particular incident, agencies will also have to consider privacy risks associated with the possibility of eventual public disclosure, including through Freedom of Information Act (FOIA) requests. It would therefore be prudent for agencies to thoroughly assess what data would require redaction or re-identification risk mitigation for retention and public disclosure when drafting data sharing policies.

Whatever technical framework or governance structure is adopted for public safety purposes, public safety use cases will inevitably interface with the frameworks adopted by related sectors, notably the healthcare sector. A recent National Academy of Medicine report recommended five leadership actions which can help promote the implementation of interoperable data sharing systems [72]. These recommendations are summarized below, with modifications for the public safety community:

1. **Commit:** Agency leadership clearly communicates the importance of data interoperability to the agency mission and establishes an agency-wide or inter-agency interoperability steering group to study and champion the issue.
2. **Identify:** The interoperability steering group documents the interoperability goals, requirements, benchmarks of success, and model use cases for data sharing, which will form the standard against which procurement requirements and product evaluation will be measured.
3. **Collaborate:** Agencies (through leadership and/or the interoperability steering group) partner with counterparts at other agencies (locally and nationally) to develop a public safety-wide data sharing strategy, including technical specifications and procurement requirements.
4. **Specify:** Agencies adopt and execute the coordinated public safety-wide procurement requirements for data sharing technologies.
5. **Assess:** Agencies monitor progress against short- and long-term benchmarks of success related to the impact of data sharing on mission outcomes.

In the following section, we describe four examples of real-world models which contain valuable insights relevant to public safety data sharing challenges. In these cases, a data sharing platform was developed in collaboration between multiple entities with shared operational goals, and the technical platform was supported by a formal agreement and/or built-in tools to implement policies governing how the system is used.

Develop Data Sharing Policies by Building on Existing Frameworks: Key Takeaways.

- Agency leaders can build momentum for data sharing efforts and leverage shared infrastructure and expertise by collaborating with state and local open data and smart city initiatives.
- Agencies should take special care to build security and privacy protections into data sharing tools to meet legal requirements, operational needs, and public concerns.
- Key features of a data sharing initiative include agency leadership commitment, clearly articulated goals, strong collaborations, coordinated procurement requirements, and regular impact assessments.

4.3.1. Virtual USA

Virtual USA (vUSA) is a program designed to establish multi-jurisdictional situational awareness via the deployment of web-based, Geographic Information System (GIS)-enabled common operating pictures and the exchange of datasets across jurisdictional boundaries to help public safety and emergency management agencies plan for, respond to, and recover from emergencies and disasters [73]. The datasets targeted by vUSA include both publicly-managed data (e.g., aerial imagery, address points, land ownership, status of critical infrastructure, transportation systems, and search and rescue teams) and privately-managed data (e.g., status of commercial communication networks, utilities, and social media feeds) [74]. Early participants in vUSA developed two regional MOUs for collections of states in the U.S. Southeast and Pacific Northwest, which evolved into a unified National Information Sharing Agreement [75]. The agreement is designed to allow data providers to maintain control over their own data at all times, with access provided through weblinks in metadata files, rather than placing data in a common repository. Signatories, who can include public and private sector entities, are responsible for enrolling and verifying their own users, and can limit access to their data to particular users if they desire. To share data provided by a different participating entity with a third party who is not a signatory to the agreement (e.g., to respond to public records requests), permission from the data provider must be obtained.

The vUSA metadata requirements are built on Federal Geographic Data Committee metadata standards. Metadata files must include a link to where actual data are stored, detailed contact information for a person associated with the dataset, and any use constraints. Acceptable metadata file types (KML, XML, KMZ, GeoRSS, REST Services, WMS, and ATOM) are based on OGC recommendations. In addition to the metadata requirements, participants agree to conform their data to open standards and adhere to a set of agreed-upon security

practices. One user summed up the value of the interoperable data access provided by vUSA succinctly: "We can use our own viewer and see everybody else's stuff."[19]

The vUSA approach of providing access to information through links to data has the advantage of restricting physical control over the data to its creator and ensuring users always access the most up-to-date records. However, it does not require the actual datasets to conform to particular data formats or schema or provide translation for datasets created in different formats. Additionally, this model could pose problems for situations without internet connectivity, where the ability to locally download data, even temporarily, may be necessary [6]. It also makes data access vulnerable to failures at source servers, which could be especially problematic during critical incidents when Internet connectivity may be degraded, infrastructure (including source servers) may be damaged, or a greater-than-normal volume of requests could overload the source server's capacity. A data sharing policy that accounts for such use cases may need to weigh the risks and benefits of more flexible data access procedures and articulate mechanisms for ensuring data access in both connected and unconnected environments.

The DHS Science and Technology Directorate (S&T) First Responder's Group is working with several partners to continue the evolution of vUSA. On a national scale, the National Information Sharing Consortium (NISC) is expanding upon vUSA tools that support operational workflows and maximize access to relevant stakeholder data. While S&T will phase out the initial Virtual Library platform, the NISC will convey its capabilities through a multi-tool environment that will include Esri's ArcGIS Online, an information sharing and mapping platform used to create interactive web maps and applications. Regionally, S&T has transitioned the Virtual Library as an operational capability used by the state and local jurisdictions that comprise the National Capital Region. Finally, S&T serves as a key partner with the White House Information Sharing and Access Interagency Policy Committee (ISA IPC) and with the Program Manager for the Information Sharing Environment (PM-ISE), which is responsible for advancing information sharing across the nation. S&T and the NISC co-chair the Incident Management Information Sharing Subcommittee of the ISA IPC and PM-ISE, thus the vUSA program also provides a platform for first responders to shape the national strategy for information sharing.

Key features of vUSA:

- **Agency control:** Agencies maintain control over their datasets and personnel credentialing.
- **Metadata standards:** Users access data through links in metadata files, which conform to standard formats.

[19] Quote from Kenny Ratliff, Kentucky Department of Military Affairs GIS manager. https://www.dhs.gov/science-and-technology/cusec-leverages-virtual-usa-video.

- **Federal link:** Managed by groups that drive national information sharing strategy development.

4.3.2. Silicon Valley Regional Data Trust

The Silicon Valley Regional Data Trust (SVRDT) is an information sharing initiative between several public service agencies (education, health, welfare, and justice) in the Silicon Valley region that serve vulnerable youth [76][20]. Because of the highly sensitive nature of the data collected by each of these agencies, the security and privacy precautions addressed by the SVRDT are highly relevant to the types of data exchanged during emergency incident response. The SVRDT was designed expressly to ensure that the data exchanged are exclusively the most critical to the participating agencies' shared goals and that all data exchanges comply with applicable laws. The development process of the SVRDT echoes several of the recommendations for agency leadership from the National Academy of Medicine described earlier to promote interoperable data sharing solutions.

The first step in developing the SVRDT was the development of an example use case, which was presented to each agency to prompt discussion about what types of data from each participating agency would be useful to exchange to achieve a positive outcome for the client. After each agency developed a list of priority data elements, a group composed of representatives from each agency selected a small number of data elements that were high priority for all agencies and used these data elements to write a series of policy and technology design principles. These principles provided a foundation for the data sharing platform and the policy framework. Policy documents (a multi-agency agreement and an enterprise MOU) incorporated privacy and security requirements based on a legal assessment of all applicable state and federal laws regarding sharing of private information, including health, criminal, and education data.

Based on the SVRDT design principle of "integration at the 'edge,'" the SVRDT data portal does not directly access individual agencies' databases, but rather each agency maintains a data environment containing only the data that they have agreed to share under the terms of the SVRDT, and it is these databases with which requests through the SVRDT data portal interact. These agency data environments are controlled by the individual agencies but housed on a network separate from their "home" network. Similarly, access to the SVRDT data portal requires role-based credentials generated by individual agencies, which determine which data elements an individual is allowed to access. The SVRDT data portal also utilizes a standardized metadata framework, which defines the SVRDT data taxonomy (naming, structure, and content). The metadata framework facilitates translating data from its native format in agency systems and satisfying queries through the SVRDT data portal.

[20] The IJIS Institute is currently working with SVRDT on the execution of the policy framework and technical infrastructure for information sharing and data management.

The SVRDT MOU describes the requirements for accessing and protecting data from the SVRDT data portal and includes provisions for sharing data with third party researchers. In addition to the collaborative, policy-focused design process, several components of the SVRDT initiative provide lessons and features that would be valuable for public safety agencies to consider when developing cross-agency data sharing programs.

Key features of the SVRDT:

- **Advisory committee:** The initiative is overseen by a committee composed of representatives from each of the participating agencies, providing governance and expertise as necessary.
- **Logging transactions:** The data portal maintains a record of data queries and exchanges, which can provide oversight and transparency (both across agencies and with the public) and support related research and evaluation.
- **Credentialing and access:** Agencies are responsible for credentialing their employees in accordance with the requirements of the information sharing agreement; SVRDT validates user credentials for each information request.
- **Agency control of data:** Agencies maintain control over the data they provide to the shared data platform and can revoke access to their data if they believe it is being used inappropriately or if a data breach has occurred.
- **Data integration:** A standardized metadata framework supports discovery and translation of data from agencies using different source formats.

4.3.3. DHS Infrastructure Protection Gateway

The Infrastructure Protection Gateway [77] is a program that allows DHS partners to access detailed infrastructure security and resilience information, including geospatial data, occupancy estimates, policy documents, and related assets and resources, as well as analysis tools characterizing risks and threat mitigation strategies. Participants include federal, state, local, territorial, and tribal government agencies and private sector partners (e.g., utility operators, industrial facilities). Users have access to infrastructure surveys and assessments, a map tool, a digital library of infrastructure information resources, and an events and incidents tool for managing data related to specific incidents.

By default, federal government users have viewing permission for all information in the Gateway, while state, local, tribal, and territorial government users have access to information within their state. Data providers can place further restrictions on their data or expand permissions to additional users as desired. Inter-agency data sharing through the Gateway can also be established through formal MOUs. Some information within the Gateway is classified as Protected Critical Infrastructure Information (PCII), which can only be shared with authorized parties. With the mapping tool, users can visualize layers such as

infrastructure protection, weather, traffic, public transit, natural hazard risks, and population data.

The policies at the foundation of the Infrastructure Protection Gateway help users share information with protection from FOIA requests, state and local disclosure laws, civil litigation, and regulatory use. If users anticipate needing access to data resources under conditions of degraded or absent network connectivity, local copies of data can be made and shared with authorized parties. The Gateway also has procedures for emergency data sharing on a short-term basis for circumstances when there is a critical need to share data beyond the predetermined access controls.

DHS's Protective Security Advisors support local communities as critical infrastructure security specialists by assessing their existing cybersecurity and ICAM procedures to help them plan for and implement integrating their resources with the Gateway. The map tool is built using Esri software and utilizes associated data standards. The Gateway also defines an infrastructure data taxonomy, which establishes a common nomenclature for infrastructure assets to facilitate inter-agency interoperability and analytics. A planned upgrade to the Infrastructure Protection Gateway is currently underway which will enhance capabilities for real-time data integration, modular data sharing platforms, and automated PCII redaction, among other features.

Key features of the Infrastructure Protection Gateway:

- **Cross-jurisdictional platform:** The Infrastructure Protection Gateway provides a shared platform of nationwide datasets and risk assessments.
- **Access policies:** Users have default data access privileges based on their level of authority/jurisdiction, but more tailored access rules can also be applied.
- **Policy protections:** The data sharing policies underlying the Infrastructure Protection Gateway shield users from legal risks and provide contingencies for special operational circumstances.
- **Agency support:** DHS assists users with cybersecurity evaluations, data integration, and ICAM procedures.

4.3.4. National Capital Region Network (NCRnet)

The National Capital Region (which includes the District of Columbia and surrounding areas in Maryland and Virginia) encompasses an extraordinary complexity of political, jurisdictional, and organizational layers of authority in its geographic area. The NCR crosses local city, county, and state boundaries, federal agencies, and autonomous transportation authorities, such the Metropolitan Washington Airports Authority (MWAA) and the Washington Metropolitan Area Transit Authority (WMATA). Law enforcement alone spans not just city, county, and state police departments and sheriffs' offices, but federal and

regional entities such as Metro Transit Police, U.S. Capitol Police, U.S. Park Police, Maryland-National Capital Park Police, and many others. This region therefore has particularly acute needs for cross-jurisdictional public safety data sharing.

The National Capital Region Network (NCRnet) [78] grew out of an initiative by the region's local government Chief Information Officers (CIOs) to interconnect their respective jurisdictional networks in support of public safety communications needs. Most local jurisdictions had their own institutional fiber optic networks supporting internal government data needs, and regional stakeholders sought to physically interconnect them and add electronics to create a resilient, interconnected network.

The system in the NCR was facilitated by NCRnet's regional architecture, which allowed stakeholders to negotiate enterprise licenses for the region rather than requiring each jurisdiction to allocate funds for their own license fees, enabling significant cost savings. Jurisdictions can also join contracts negotiated by other NCRnet partners rather than initiating a new contract for the same product or service. Data exchange policies are implemented with multiprotocol label switching, which allows application administrators to assign rules to data types specifying allowed recipients, retention dates, and the like.

Certain critical data applications run over NCRnet exclusively while others co-exist on both the NCRnet and the public Internet. CAD2CAD was one of the first applications to run on NCRnet; it links CAD systems in local jurisdictions to each other so they can automatically dispatch the closest available fire department resource automatically, regardless of jurisdictional boundaries. CAD2CAD replaced a system of phone calls, reducing cross-jurisdiction dispatch times from many minutes to only seconds.

A second application that takes advantage of NCRnet's unique design is the secure video exchange application, which integrates real-time video data from various siloed camera networks across the region. An integration tool was built to ingest video data in a variety of native formats (including file types, compression algorithms, and bandwidths) and translate all video streams into a single format, which is accessible to NCRnet users. End users are then able to apply their preferred protocols for viewing standardized video streams on their own video platforms. The purpose of the integration tool is to mitigate overloading servers hosting video streams from heavy pull request traffic and to protect networks receiving video data by channeling all data streams through a "neutral territory" rather than connecting end users directly to a data source.

The NCRnet now includes twenty-one local jurisdictions, MWAA, WMATA, and some federal agencies, and supports a variety of applications that seamlessly exchange data across participating agencies such as License Plate Reader, Geolocated Index Exchange, Automated Fingerprint Index System, Mugshots Exchange, and many others.

The governance and oversight of NCRnet is facilitated by the organization of the Metropolitan Washington Council of Governments (MWCOG). NCRnet users leverage the

MWCOG Framework for coordination efforts, including federal grants. Under this Framework, a Homeland Security Executive Council (HSEC) consisting of executive leaders in the region sets funding priorities and determines public safety and emergency response objectives and goals. MWCOG committees (standing multidisciplinary task forces and working groups) are responsible for various areas of emergency response; they sponsor projects and oversee programs in support of their jurisdiction and associated regional objectives.

NCRnet is overseen by the CIO Committee which, in turn, uses several subcommittees (Chief Information Security Officers, network managers, GIS administrators) to oversee and guide the CIO programs. HSEC has developed a master data sharing framework, policies, and operational procedures to enable NCRnet operations, but governance and security of application systems are handled by application administrators. Administrators often develop their own data exchange agreements specific to the particular application and its users, which then become addenda to the data sharing agreement.

Key features of NCRnet:

- **Design principles:** Built for high resilience, high capacity, high security, and high risk transparency.
- **Cross-jurisdictional collaboration:** Leverages a regional political body (MWCOG) to bring together leaders from relevant jurisdictions and authorities.
- **Infrastructure and policy collaboration:** Participation entails physical interconnection of network infrastructure and data sharing governance agreements for both enterprise and application-specific functionalities.
- **Economies of scale:** Supports cost savings by sharing infrastructure and technology acquisition expenses.

4.4. Engaging with the Broader Public Safety Community on Data Sharing Solutions

While agencies embark on the routes to data sharing interoperability described above, they can also help lay the foundation for public safety-wide solutions and frameworks developed and certified by entities with convening power and, potentially, authority. Such a coordinated approach will help the public safety community to share resources and learn from the experiences of agencies in a wide variety of contexts. Inter-disciplinary and -jurisdictional groups can assess the community at a systems level and perform evaluations to quantify the impacts of data interoperability initiatives [e.g., 79]. The groups and organizations below share an interest in leading the public safety community towards data interoperability and would benefit from practitioner input on existing and desired data sharing use cases and policy preferences.

National Public Safety Telecommunications Council (NPSTC). NPSTC is a practitioner-driven organization that convenes users, technology developers, and other experts to evaluate the benefits and challenges of various public safety communications technologies, and advocates on behalf of the public safety community through white papers, reports, and public comments to government authorities such as the Federal Communications Commission. Interoperability is a core focus area across the NPSTC working groups, some of which have begun addressing issues around data exchange interoperability directly. For example:

- The EMS Working Group has compiled a list of broadband applications for EMS, including a standard application programming interface for interoperable exchange of patient care records, which the working group notes is critical to the interoperability of many of the applications on their list [80].
- The Video Technology Advisory Group connects the NPSTC community with the video technology research, development, and evaluation work related to video applications conducted by DHS and PSCR, such as the DHS report on video policy considerations for public safety [60].
- The Public Safety Internet of Things (IoT) Working Group has developed a series of IoT use cases to explore the potential value and challenges of implementing networked sensors and automated data analytics in fire, EMS, and law enforcement operations [81].

A key challenge recognized by the IoT Working Group is the fact that commercially-available IoT sensors are generally built on proprietary data exchange standards, meaning that each solution product comes with a siloed integration, visualization, and analytics system, which cannot exchange data with another vendor's system. If an agency wishes to acquire such solutions individually, they will need to manage separate systems with separate dashboards and integration platforms for each product from a different vendor, and data analytics features cannot leverage data generated by other vendors' devices. Many IoT use cases (such as gunshot detection sensors, vehicle tracking systems, and biometric monitors) offer value through enhanced situational awareness and contribute to a common operating picture; therefore, integrating multiple data streams into a single system for visualization, alerting, and analytics is critical for public safety use cases. NPSTC working groups regularly address governance issues in their work products. For example, to promote nationwide coordination in the naming of mission critical push-to-talk talkgroups, NPSTC recommended that states collaborate to create blueprints for interoperable talkgroup management [82]. Engaging in the discussions within these and other NPSTC working groups on data exchange interoperability will help public safety agencies explore the possibilities of data sharing applications and discuss the real-world risks and benefits of different technical and policy interoperability approaches. Since commercial solutions are evolving rapidly, having these discussions as early as possible will help keep the practitioner community aware of technological developments, provide critical feedback, and potentially

reach consensus about their preferred solutions or requirements. A unified position from the practitioner community will communicate to technology developers what their users expect and demand of these emerging technologies.

SAFECOM-NCSWIC. The DHS SAFECOM program serves a convening function for the public safety community by organizing working groups on topics of communications technology and cross-jurisdictional governance. SAFECOM publishes grant guidance and white papers to assist public safety agencies in understanding and implementing communications technologies. SAFECOM meetings and working groups include representatives of organizations in traditional and adjacent public safety sectors, as well as representatives of federal agencies and technology vendors. SAFECOM also works in collaboration with the NCSWIC, as described in Sec. 3.3. SAFECOM's ICAM working group has worked closely with the developers of the Trustmark Framework, and is developing guidance documents to help agency leaders and IT managers implement the framework with public safety-specific Trust Interoperability Profiles. Interoperability of emerging data sharing technologies is an area of interest for the SAFECOM community; therefore, public safety agencies have an opportunity to contribute to discussions surrounding possible guidance documents from SAFECOM on data exchange standards and other technical requirements, as well as governance structures and implementation best practices. The SAFECOM program also recently conducted a survey of public safety agencies to characterize community needs and experience regarding the technical, operational, and governance aspects of communications technologies [83]. Therefore, this is an opportune time for practitioners to help develop national guidance and recommendations for public safety data sharing applications by engaging with the SAFECOM program.

First Responder Network Authority (FRNA). The NPSBN (FirstNet) overseen by the FRNA offers an unprecedented opportunity for the public safety community to shape the interoperability requirements for emerging data sharing technologies. Every U.S. state and territory has a SPOC with the FRNA, who can serve as a liaison between local public safety agencies and the national authority. Agencies can also engage with members of FirstNet's Public Safety Advisory Committee (PSAC), which represents the views of the first responder community to the FRNA. The existence of a dedicated Long-Term Evolution (LTE) network for public safety agencies will avoid many of the technical obstacles facing legacy LMR networks, such as the lack of interoperability between an agency using an 800 MHz system and a neighboring agency using an ultra-high frequency system. Because of the 3rd Generation Partnership Program (3GPP) standards that are the foundation of all LTE networks, any public safety LTE network will be functionally interoperable from the physical to the transport layer for voice communications. However, it is unclear if 3GPP will develop standards for interoperability at the application layer, since these would necessarily be very context-specific (hence the variety of public safety-specific data exchange standards described in Sec. 3.1.1 and Appendix B). The law authorizing the FRNA states that it is required to "promote competition...by requiring that equipment for use on the network be

built to open, non-proprietary, commercially available standards" [84]. Therefore, the public safety community has an opportunity to communicate to the FRNA their specific interoperability needs and preferences regarding data exchange standardization in order to support the successful implementation of the NPSBN.

These are only a few examples of the groups that individual agencies can leverage in order to engage with the broader public safety community as it addresses the issue of interoperable data sharing. For public safety agencies in regions with existing interoperable communications alliances, such as NCRnet (described in Sec. 4.3.4) or the Bay Area or Los Angeles Regional Interoperable Communications Systems (BayRICS and LA-RICS, respectively), or similar regional entities, these bodies can potentially also facilitate coordination on personnel education, training, standards requirements, and purchasing decisions. Public safety practitioners can also serve as subject matter experts for the various technical bodies drafting data exchange standards, such as OASIS, APCO, and NENA, as well as SDOs and other organizations in related fields. For example, the Organization of Scientific Area Committees (OSAC), a NIST-administered program, facilitates the development of voluntary consensus standards for forensic science. OSAC is comprised of over 500 volunteer members including federal, state and local government forensic science service providers, researchers, statisticians, measurement scientists, quality managers, lawyers, judges, and representatives from the private sector. Since forensic data is an important part of many public safety operations, coordinating with the forensic science community is an important objective of public safety data sharing interoperability efforts.

On the local level, agencies can partner with neighboring agencies with whom they regularly participate in mutual aid, or with whom they see mutual benefit in sharing incident data, to brainstorm technical and policy interoperability challenges and preferences, and plan exercises to test the implementation of specific technologies and governance structures. The full scope of potential partners for agencies committed to pursuing data sharing interoperability is vast (Fig. 7). As emphasized in Sec. 4.3, strong support from agency leaders for such initiatives is critical to their success. Public safety data sharing technology advancements are only possible with engagement and collaboration across the stakeholder community, and the more this effort is driven by the needs and real-world experiences of practitioners, the more successful the outcomes will be.

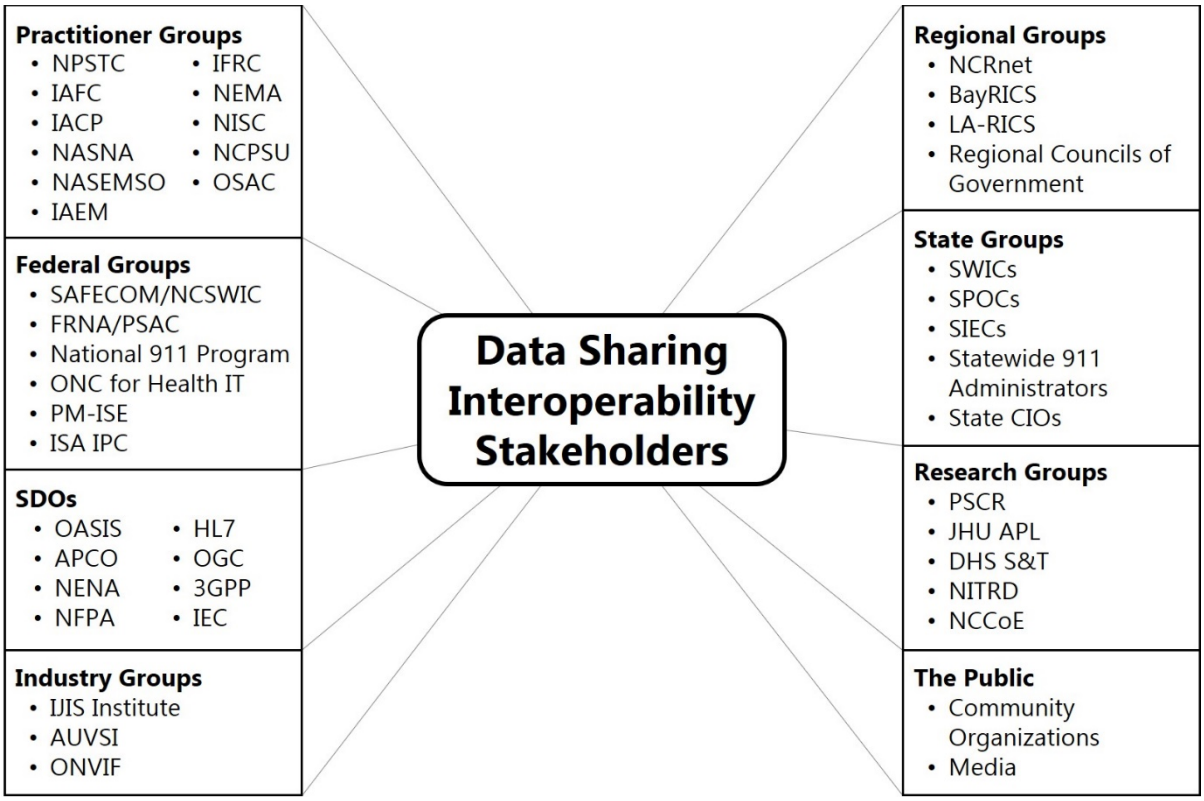


Fig. 7. Data sharing interoperability stakeholders

Agencies and other public safety entities pursuing data sharing interoperability can form partnerships with a wide range of stakeholders across different sectors (groups shown here are only representative examples). See Glossary for acronym definitions.

Engaging with the Broader Public Safety Community on Data Sharing Solutions: Key Takeaways.

- Agencies can influence and leverage groups actively working on data sharing interoperability solutions and frameworks, including NPSTC, SAFECOM, NCSWIC, and FRNA.
- Existing regional interoperability alliances, such as NCRnet, LA-RICS, and BayRICS, can serve as examples for agencies wishing to build a data sharing initiative.
- Technical bodies, including researchers and SDOs, need input from public safety leaders and first responders to ensure technologies are developed based on the operational, financial, and policy requirements of public safety users.

5. Conclusions and Recommendations

The public safety community is poised to undergo a revolution in wireless communication technology similar to the one that has transformed the commercial market over the past ten

years. Emerging data sharing applications for public safety agencies can benefit tremendously from the nationwide scale of commercial and safety-specific LTE (and soon 5G[21]) networks, which stands in contrast to the localized LMR networks and non-interoperable CAD systems utilized by public safety agencies today. Yet, the degree of interoperability provided by broadband data sharing products currently extends only to the ability to exchange bits and bytes between LTE-enabled devices; whether the software programs analyzing and visualizing these data use mutually intelligible data formats is not guaranteed. If this persists, public safety agencies that adopt these technologies will find their personnel unable to rely on them in everyday operations, such as when a fire department needs to access state property records, as well as in the most complex response scenarios—those which require real-time information sharing across jurisdictional and disciplinary boundaries.

Standardization challenges of legacy communication technologies provide a cautionary tale of how interoperability could proceed with broadband data sharing technologies. The obstacles to seamless interoperability of real-time data sharing require not just technical solutions but coordinated governance and collaboration across public safety disciplines and jurisdictions and with technology developers.

Two significant technical challenges will affect the ability of agencies to seamlessly share real-time incident data across jurisdictions. The first is the lack of widely accepted or implemented data exchange formats. Several initiatives have tackled this problem but have not yet resulted in widespread awareness by the public safety practitioner community or the technology developer community. As a result, products available to agencies today have little to no standardization of data formats. This means that agencies can only share real-time incident data with other agencies using the same product from the same vendor. Accepting this landscape, agencies who wish to share data can either coordinate to adopt the same products or choose the products they prefer and then integrate their systems using gateways or translation products. **These solutions are not sustainable if data sharing platforms are ever to be flexible enough to add new users and agencies across boundaries as incidents require.** Such approaches also carry significant financial risks from the need to maintain purpose-built interfaces and the reliance on a small number of vendors for siloed technology packages.

The second technical challenge lies in developing interoperable data access control systems. Data sharing platforms that require manual credentialing of new users with different technical architectures between different agencies will significantly inhibit such technologies from providing their maximum potential operational value. If instead agencies could leverage a public safety-wide federated identity and access control system, they would not have to

[21] 5G, or 5th Generation, is the next-generation of mobile networks using higher frequencies, bandwidths, and data upload and download speeds relative to 4G/LTE networks [85]. International standards for 5G are still under development and the final specifications may be different from the current definition.

devote precious time and attention during incidents to evaluating what level of access to provide to every person outside their agency who responds to an incident. **Interoperable access control models exist, and efforts like the Trustmark Initiative demonstrate that the public safety community is actively pursuing such solutions.** The implementation of interoperable access control systems will be critical to the success of public safety data sharing technologies.

The public safety community in the U.S. operates under a highly localized governance structure. Agencies are primarily supported by municipal, county, or state funds, and most laws and policies governing their activities are created at the local government or individual agency level. This is a logical arrangement in the sense that each agency serves its community directly and is therefore dependent on and accountable to their community. However, this decentralized structure can be an obstacle to effective incident response when more complex incidents require coordination across agencies. Furthermore, it inhibits cross-agency collaboration and long-term planning for technology implementation. This has resulted in past struggles to standardize communications technology for LMR and CAD systems and may reduce the utility of emerging broadband data sharing technologies moving forward.

This report highlights how national-level bodies can support agencies by providing leadership and guidance on standards and best practices for data sharing technologies. But this work will take time, and many agencies will not choose to wait for a perfect road map before implementing these technologies. For those agencies, this report describes key aspects of data sharing policies that agencies should consider as they adopt technologies and build data sharing collaborations with other agencies. **Data ownership and retention are among the most important factors, as they affect the support structures agencies will need to manage their growing data repositories (cloud server storage, IT managers, etc.), as well as the legal implications of collecting and disseminating various types of data.** Developing such policies will help agencies refine the vision for their data sharing objectives and build a framework that can be leveraged to expand into new partnerships and data sharing activities.

Finally, the public safety community must consider the financial risks for agencies of accepting data sharing technologies that are not built with open data exchange standards. While there is some cost for technology developers to design or upgrade a product to conform with a standard, the costs and risks to agencies of non-standardized data sharing systems are significant. **The limitations of non-standardized data sharing systems will grow as the systems become more enmeshed in an agency's daily operations, as will the costs of switching to a different system.** Agencies should therefore require that vendors meet the maximum possible level of data sharing interoperability when procuring new technologies and, if products meeting such specifications are not available, carefully evaluate the long-term costs of investing in non-interoperable technologies. Technology developers

may wish to reflect any standards conformance costs in the prices of their products; however, financially disincentivizing interoperability will encourage agencies to adopt products with reduced functionality or forgo valuable technologies altogether. This would be regrettable, as agencies would miss out on tools that improve their operations and the community, as a whole, would be hampered from realizing the full benefits of a *nationwide* broadband network.

This report highlights the approaches agencies can take to promote data sharing interoperability in both the short and the long term. In the short term, inter-agency partnerships may choose to adopt common applications or procure cross-application gateways or translators to integrate their non-interoperable applications. Although this may be an expedient approach, it does not provide actual data interoperability between systems and it could lead to unsustainable costs related to maintenance (in the case of gateways) and lock-in to a single vendor's products, and it may inhibit the expansion of new inter-agency partnerships (Fig. 6). In the long term, the public safety community must collaboratively discuss, test, and evaluate interoperability specifications that meet their shared needs for cross-agency data sharing.

Recommendations for agencies. Fully addressing the challenges discussed in this report requires concerted effort across the public safety community. Efforts are required that exceed the scope of individual agencies, but there are actions agencies can take to build their internal and regional capacity for interoperable data sharing. These include:

1. **Leverage RFP requirements.** Clearly specify data sharing interoperability requirements in RFPs, including any performance metrics related to the application of relevant standards recommended by bodies such as SAFECOM and the National 911 Program. Guidance such as SAFECOM's to encourage EDXL conformance can be leveraged even if the given procurement is not funded by a SAFECOM grant. Wherever possible, include specific interoperability requirements and any use cases of high value for the agency, such as the ability to share certain types of information with neighboring agencies and among all components of the emergency communications ecosystem. Agencies can articulate these requirements today, to the extent that they know their needs and that technology providers are able to produce the products and services agencies desire. In most areas, however, specifying data sharing interoperability requirements will require additional research and discussion among public safety stakeholders.
2. **Participate in ICAM solution development.** Engage with groups studying federated identity management and access control approaches for public safety software systems, such as the SAFECOM ICAM working group. Once satisfactory federated ICAM tools are available, agencies should include in their RFPs interoperability requirements for credential mutual intelligibility and automated personnel authorization for users from other agencies.

3. **Develop inter-agency data sharing partnerships.** Build inter-agency commissions, task forces, working groups, etc., charged with identifying the agencies' collective data sharing interoperability goals, requirements, benchmarks of success, and model use cases. These bodies may begin through existing inter-agency relationships but would ideally expand over time to collaborate across larger geographic areas and disciplinary boundaries. As consensus emerges around particular technologies and use cases, these groups could coordinate to develop a public safety-wide data sharing strategy, articulating technical specifications and procurement requirements. The data sharing strategy would serve as the foundation for a cross-agency data sharing policy, which could serve as a template for other agencies. These groups would help agencies to explore data interoperability and policy challenges together rather than in silos and would act as a unified voice to articulate practitioner needs to technology developers. To maximize the potential for success, these groups should have clear support from agency leadership, including necessary costs (salary, travel, etc.), and consist of members who exert influence on their agency's technology purchasing decisions.
4. **Collaborate with the broader public safety community.** While building local and regional inter-agency capacity, agencies should engage with national and international public safety entities, including state and federal bodies, practitioner organizations, research groups, industry groups, SDOs, nongovernmental organizations, and others (Fig. 7), to share ideas, concerns, resources, and preferences for data sharing technologies across the public safety community. This engagement should be bi-directional, with agencies providing their experiences adopting data sharing products and governance structures and national bodies sharing insights and recommendations from other practitioners, domains, and stakeholders.
5. **Make the case for investments in data sharing.** Agencies adopting data sharing tools can derive benefit from their data outside of operational contexts. With planned monitoring and evaluation metrics, agencies can analyze their own data use and data sharing patterns to quantitatively understand where data sharing has the most significant impact and where additional data sharing capabilities might be useful. This can help agencies make improvements to their data sharing operations and make evidence-based arguments regarding future investments in data sharing resources.

These recommendations recognize that no two public safety agencies in the country are identical when it comes to their readiness to adopt data sharing technologies and engage in the process of developing interoperability solutions. The unique needs and perspectives of different agencies underscores the value of learning from other agencies and coordinating as much as possible to find solutions and develop best practices.

Recommendations for the entire public safety communications community. To reach an ideal future state of fully interoperable real-time data sharing, the public safety community needs to work in a collaborative, coordinated fashion to tackle multiple aspects of the data

interoperability challenge simultaneously. Based on the lessons learned from past public safety communications technology interoperability challenges, ongoing trends in emerging technologies, and examples from other sectors highlighted in this report, we recommend two key actions for the public safety community.

Community Recommendation 1: Prioritize funding for data integration tools and data sharing governance work

Entities that offer grants and other funding for public safety communications technology should devote a dedicated portion of their available funds to tools and activities that explicitly advance data sharing interoperability. Two key areas that warrant increased resources are (1) the development of tools capable of integrating data from a variety of sources in different native formats and converting the data into specific open formats that can be understood by other platforms, and (2) costs associated with engaging in data sharing initiatives, such as salaries and travel to standards development and governance meetings. Materially supporting this work is critical to ensuring that it is a high priority for the public safety community and that participation is not restricted to only those agencies and organizations with budget to spare.

Community Recommendation 2: Establish a community-wide public safety data sharing task force to develop governance resources and a framework for data sharing interoperability requirements

This task force needs broad stakeholder participation, including representatives from public safety agencies, federal partners, practitioner organizations, SDOs, technology developers, and researchers. The participants in this task force should be champions of data sharing within their organizations and exert influence on their organization's decision-making processes. They should represent a range of expertise including technical, economic, and governance issues in the public safety community, including past and ongoing data exchange standards development; software performance and conformance testing practices; cybersecurity; technology procurement, acquisition, and grant-making; the roles of a wide range of relevant stakeholder organizations; public safety operational requirements; technology research developments; and the public safety technology market. The primary objectives of this task force would be to develop template language for data sharing policies, RFPs, and contracts and a public safety data sharing framework. Template language is critical for facilitating implementation of interoperable, secure data sharing capabilities for the full range of public safety agencies across the country. The public safety data sharing framework would address at least three key issues:

1. Baseline data elements which must be standardized,
2. Preferred/required data exchange standards for these data elements, and
3. Reference implementations for vendors and users to demonstrate and test technologies.

Such a framework could provide the foundation for additional resources, such as simple comparison metrics of standards conformance and cybersecurity specifications of different products, similar to the Consumer Reports Digital Standard [86].

By simultaneously tackling the technical, governance, and economic aspects of data sharing interoperability, the public safety community has the opportunity to maximize the benefits made possible by the creation of a nationwide public safety broadband network.

Acknowledgments

The authors thank the following individuals for contributing their expertise to this report:

Michael Alagna, IJIS Institute
Anu Appaji, First Responder Network Authority
John Beltz, National Institute of Standards and Technology
Lotfi Benmohamed, National Institute of Standards and Technology
Rex Brooks, OASIS Emergency Management Technical Committee
John Contestabile, Johns Hopkins University Applied Physics Laboratory
Michael Dent, County of Fairfax, Virginia
Matthew Dowd, County of Fairfax, Virginia
Bill Fisher, National Institute of Standards and Technology
Laurie Flaherty, National 911 Program
Barry Fraser, National Public Safety Telecommunications Council
John Garofolo, National Institute of Standards and Technology
Tim Grapes, IJIS Institute
Pete Hallenbeck, Efland Volunteer Fire Department
Elysa Jones, OASIS Emergency Management Technical Committee
Karla Jurrens, Texas Department of Public Safety
Alison Kahn, National Institute of Standards and Technology
Chris Kindelspire, Grundy County Emergency Telephone Service Board
Rick Kuhn, National Institute of Standards and Technology
Barry Luke, National Public Safety Telecommunications Council
Jennifer Marshall, National Institute of Standards and Technology
Gabriel Martinez, Department of Homeland Security
Sean McSpaden, National Information Sharing Consortium
Ricky Morgan, Department of Homeland Security
Matt Moyer, Georgia Tech Research Institute
Chris Nelsen, National Institute of Standards and Technology
Dave Nolan, Department of Homeland Security
Michael Ogata, National Institute of Standards and Technology
Niki Papazoglakis, Mobility 4 Public Safety
Gregoor Passchier, National Information Sharing Consortium
Davide Pesavento, National Institute of Standards and Technology
Ryan Poltermann, Commdex
Jeff Posner, First Responder Network Authority
Rajan, First Responder Network Authority
Sam Ray, National Institute of Standards and Technology
Ziggy Rivkin-Fish, CTC Technology & Energy
Laurence Ruhf, County of Fairfax, Virginia

Bill Schrier, First Responder Network Authority
David Van Ballegooijen, Western Fire Chiefs Association
Jared Vandenheuvel, Texas Department of Public Safety
John Wandelt, Georgia Tech Research Institute
Jeff Waters, OASIS Emergency Management Technical Committee
Charles Werner, National Council on Public Safety UAS

References

[1] FirstNet Public Safety Advisory Committee (2014) Use Cases for Interfaces, Applications, and Capabilities for the Nationwide Public Safety Broadband Network. Available at https://2014-2018.firstnet.gov/sites/default/files/PSAC%20Use%20Cases%20Report.pdf

[2] Contestabile JM (2011) Concepts on Information Sharing and Interoperability. *Domestic Preparedness*. Available at https://www.domesticpreparedness.com/preparedness/concepts-on-information-sharing-and-interoperability

[3] Rhodes C (2015) The four definitions of interoperability. Available at https://healthcareit.me/2015/04/07/the-four-definitions-of-interoperability

[4] Garofolo JS, Contestabile J, Powell J, Corso JJ, Friedland G, Tu P, Pankanti S, Brush L, Frost E, Zoufal D, Luke B, Surfaro S, Hoogs A, Audia J, Garfinkel S, Schwartz R, Weinert A (2017) First Workshop on Video Analytics in Public Safety. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency/Internal Report (NISTIR) 8164. Available at https://www.nist.gov/publications/first-workshop-video-analytics-public-safety

[5] Harris County Central Technology Services (2017) Super Bowl LI: FirstNet After Action Report. Available at https://hclte.harriscountytx.gov/Documents/SBLI%20FirstNet%20AAR%20Final.pdf

[6] National Alliance for Public Safety GIS Foundation, U.S. Department of Homeland Security (2017) National Mutual Aid Technology Exercise: After-Action Report and Improvement Plan. Available at https://www.napsgfoundation.org/wp-content/uploads/2018/01/FINAL_NMATE_AAR_20171231_Final.pdf

[7] Dickson RL, Patrick CB, Crocker K, Ward BT, Gleisberg GR (2017) Improving Systems of Care in Time-Sensitive Emergencies. *Journal of Emergency Medical Services* 42(1). Available at https://www.jems.com/articles/print/volume-42/issue-1/features/improving-systems-of-care-in-time-sensitive-emergencies.html?c=1

[8] U.S. Department of Homeland Security (2019) *SAFECOM Interoperability Continuum*. Available at https://www.dhs.gov/sites/default/files/publications/interoperability_continuum_brochure_2_1.pdf

[9] Organization for the Advancement of Structured Information Standards (2017) OASIS Emergency Management TC. Available at https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=emergency

[10] National Information Exchange Model (2018) *NIEM Releases*. Available at http://niem.github.io/niem-releases/

[11] Association of Public-Safety Communications Officials-International, National Emergency Number Association (2017) *APCO NENA 2.105.1-2017: NG9-1-1 Emergency Incident Data Document (EIDD).* Available at https://cdn.ymaws.com/www.nena.org/resource/resmgr/standards/APCO_NENA_2.105.1-2017_EIDD_.pdf

[12] National Fire Protection Association Technical Committee on Data Exchange for the Fire Service (2015) NFPA 950: Standard for Data Development and Exchange for the Fire Service. Available at https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=950

[13] OASIS Emergency Management Technical Committee (2018) *Emergency Data Exchange Language (EDXL) Technical Documents*. Available at http://docs.oasis-open.org/emergency/

[14] NIEM Success Stories (2018) Available at https://www.niem.gov/about-niem/success-stories

[15] National Emergency Number Association (2018) *EIDD& IDX Frequently Asked Questions, NENA-REF-011.1-2018.* Available at https://cdn.ymaws.com/www.nena.org/resource/resmgr/standards/NENA-REF-011.1-2018_EIDD_&_I.pdf

[16] National 911 Program (2017) National 911 Progress Report. Available at https://www.911.gov/project_national911progressreport.html

[17] National Fire Protection Association Technical Committee on Data Exchange for the Fire Service (2016) NFPA 951: Guide to Building and Utilizing Digital Information. Available at https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=951

[18] U.S. Department of Homeland Security (2018) Next Generation First Responder Integration Handbook. Available at https://www.dhs.gov/science-and-technology/ngfr/handbook

[19] Grassi P, Fisher B, Jha S, Kim W, McCorkill T, Portner J, Russell M, Umarji S (2018) Mobile Application Single Sign-On: Improving Authentication for Public Safety First Responders. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 1800-13, Draft for public comment. Available at https://www.nccoe.nist.gov/publication/1800-13/index.html

[20] Fisher B, Brickman N, Burden P, Jha S, Johnson B, Keller A, Kolovos T, Umarji S, Weeks S (2017) Attribute Based Access Control. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 1800-3, Rev. 2, Draft for public comment. Available at https://www.nccoe.nist.gov/projects/building-blocks/attribute-based-access-control

[21] Choong Y, Dawkins S, Furman S, Greene KK, Prettyman SS, Theofanos M (2018) Voices of First Responders – Identifying Public Safety Communication Problems: Findings from User-Centered Interviews Phase 1, Volume 1. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency/Internal Report (NISTIR) 8216. Available at https://doi.org/10.6028/NIST.IR.8216

[22] U.S. Office of the Director of National Intelligence Program Manager for the Information Sharing Environment, U.S. Department of Homeland Security, International Association of Chiefs of Police (2015) Recommended Principles and Actions Report. *Identity, Credential, and Access Management: Wireless Mobility in Law Enforcement, Justice, and Public Safety National Strategy Summit, 8-9 Oct. 2014* (Washington, D.C.). Available at https://www.dni.gov/files/ISE/documents/DocumentLibrary/ICAM_Summit_Report.pdf

[23] National Fallen Firefighters Foundation (2016). *Fire Service Technology Summit* (Oakland, CA). Available at https://www.firerescuemagazine.com/content/dam/fe/downloads/FFN-FRM-Downloads-Editorial/tech-report-012517.pdf

[24] Samarati P, de Vimercati SC (2001) Access Control: Policies, Models, and Mechanisms. *Foundations of Security Analysis and Design*, Lecture Notes in Computer Science., eds Focardi R, Gorrieri R (Springer Berlin Heidelberg), pp 137–196.

[25] Tripunitara MV, Li N (2007) A theory for comparing the expressive power of access control models. *Journal of Computer Security* 15(2):231–272. https://doi.org/10.3233/JCS-2007-15202

[26] Sandhu R, Bhamidipati V, Munawer Q (1999) The ARBAC97 Model for Role-based Administration of Roles. *ACM Transactions on Information and System Security* 2(1):105–135. https://doi.org/10.1145/300830.300839

[27] Microsoft Corporation (2018) Active Directory Domain Services. Available at https://docs.microsoft.com/en-us/windows/desktop/ad/active-directory-domain-services

[28] Oracle Corporation (2013) Using Active Directory for Authentication and RBAC of Management Services. Available at https://docs.oracle.com/cd/E39820_01/doc.11121/gateway_docs/content/general_rbac_ad_ldap.html

[29] Oracle Corporation (2019) Access Control with Oracle User Management. Available at https://docs.oracle.com/cd/E18727_01/doc.121/e12843/T156458T185608.htm

[30] U.S. Federal Emergency Management Agency (2017) *National Incident Management System Guideline for the National Qualification System*. Available at https://www.fema.gov/media-library-data/1523470612203-906948554492c1f2663c9e69eb636401/NIMS_NQS_Guideline_April2018.pdf

[31] Hu VC, Ferraiolo D, Kuhn R, Schnitzer A, Sandlin K, Miller R, Scarfone K (2014) Guide to Attribute Based Access Control (ABAC) Definition and Considerations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-162. https://doi.org/10.6028/NIST.SP.800-162

[32] Organization for the Advancement of Structured Information Standards (2013) *eXtensible Access Control Markup Language (XACML) Version 3.0.* Available at http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.pdf

[33] Ferraiolo D, Chandramouli R, Kuhn R, Hu V Extensible Access Control Markup Language (XACML) and Next Generation Access Control (NGAC). *Proceedings of the 2016 ACM International Workshop on Attribute Based Access Control, 9-11 Mar. 2016* (New Orleans, LA), pp 13–24. https://doi.org/10.1145/2875491.2875496

[34] DeTreville J (2002) Binder, a logic-based security language. *Proceedings of the 2002 IEEE Symposium on Security and Privacy*, SP '02. (IEEE Computer Society, Washington, D.C.), p 105. Available at https://dl.acm.org/citation.cfm?id=830540

[35] Jiang H, Bouabdallah A (2017) JACPoL: A Simple but Expressive JSON-based Access Control Policy Language. *WISTP IFIP 11th International Conference on Information Security Theory and Practice* (Springer Verlag, Heraklion, Greece), pp 1–17. Available at https://www.researchgate.net/publication/320407190_JACPoL_A_Simple_but_Expressive_JSON-based_Access_Control_Policy_Language

[36] García-Crespo Á, Gómez-Berbís JM, Colomo-Palacios R, Alor-Hernández G (2011) SecurOntology: A semantic web access control framework. *Computer Standards and Interfaces* 33(1):42–49. https://doi.org/10.1016/j.csi.2009.10.003

[37] Pilz A (2004) "Policy-Maker": a toolkit for policy-based security management. *2004 IEEE/IFIP Network Operations and Management Symposium (IEEE Cat. No.04CH37507)* (Seoul, South Korea), Vol. 1, pp 263–276. https://doi.org/10.1109/NOMS.2004.1317664

[38] Blaze M, Feigenbaum J, Ioannidis J, Keromytis A (1999) *The KeyNote Trust-Management System Version 2 (IETF RFC 2704).* Available at https://tools.ietf.org/html/rfc2704

[39] Li N, Mitchell JC (2003) RT: a Role-based Trust-management framework. *Proceedings DARPA Information Survivability Conference and Exposition* (IEEE, Washington, D.C.), Vol. 1, pp 201–212 vol.1. https://doi.org/10.1109/DISCEX.2003.1194885

[40] Agarwal S, Sprick B, Wortmann S (2004) Credential Based Access Control for Semantic Web Services. *American Association for Artificial Intelligence Spring Symposium*, pp 44–51. Available at http://www.aaai.org/Papers/Symposia/Spring/2004/SS-04-06/SS04-06-007.pdf

[41] Harrison MA, Ruzzo WL, Ullman JD (1976) Protection in operating systems. *Communications of the ACM* 19(8):461–471. https://doi.org/10.1145/360303.360333

[42] Li N, Mitchell JC (2003) Datalog with Constraints: A Foundation for Trust Management Languages. *Practical Aspects of Declarative Languages. PADL 2003. Lecture Notes in Computer Science*, eds Dahl V, Wadler P (Springer, Berlin, Heidelberg), Vol. 2562, pp 58–73. https://doi.org/10.1007/3-540-36388-2_6

[43] Moyer M, Wandelt J, Goldstein S, Krug J, Lee B, Roth S, Taylor D, Reddick EA (2016) *Enabling Scalable Multidimensional Trust in Heterogeneous Distributed Systems with Machine-Readable Trustmarks*. Available at https://trustmark.gtri.gatech.edu/wp-content/uploads/2017/09/trustmark-white-paper.pdf

[44] U.S. Department of Homeland Security, National Council of Statewide Interoperbility Coordinators (2017) *Position Paper: Endorsing the Trustmark Framework.* Available at https://www.dhs.gov/sites/default/files/publications/ICAM%20WG%20Trustmark%20Framework%20Position%20Paper_FINAL%20Approved508v2.pdf

[45] National Public Safety Telecommunications Council (2017) *Trustmark Framework Position Paper*. Available at http://www.npstc.org/download.jsp?tableId=37&column=217&id=3959&file=ICAM_NPSTC_Position_Paper_170717.pdf

[46] International Association of Chiefs of Police (2017) *Adopted Resolution: Nationwide Adoption of Identity, Credential, and Access Management Services and the Trustmark Framework.* Available at https://dnn9ciwm8.azurewebsites.net/Portals/0/documents/pdfs/Communications/IACP_Resolutions_2017_Final.pdf

[47] Joint Task Force Transformation Initiative (2015) Security and Privacy Controls for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 4. Available at https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final

[48] U.S. Department of Justice Federal Bureau of Investigation (2018) *Criminal Justice Information Services (CJIS) Security Policy, v. 5.7.* Available at https://www.fbi.gov/file-repository/cjis-security-policy_v5-7_20180816.pdf/view

[49] U.S. Department of Health and Human Services (2015) The HIPAA Privacy Rule. Available at https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

[50] Eurich M, Burtscher M (2014) The Business-to-Consumer Lock in Effect. *Cambridge Service Alliance*. Available at https://cambridgeservicealliance.eng.cam.ac.uk/resources/Downloads/Monthly%20Papers/2014AugustPaperBusinesstoConsumerLockinEffect.pdf

[51] National Information Sharing Consortium (2015) Local First Responder Decision Support Project Findings Report. Available at https://www.nisconsortium.org/wp-content/uploads/2016/04/Project-Findings-Report.pdf

[52] Association of Public-Safety Communications Officials-International (2018) Interoperability & SIECs. Available at https://www.apcointl.org/spectrum-management/spectrum-management-resources/interoperability/siecs/

[53] U.S. Department of Transportation Federal Aviation Administration (2019) Unmanned Aircraft Systems: Public Safety and Government. Available at https://www.faa.gov/uas/public_safety_gov/

[54] National Conference of State Legislatures (2018) Current Unmanned Aircraft State Law Landscape. Available at http://www.ncsl.org/research/transportation/current-unmanned-aircraft-state-law-landscape.aspx

[55] National Public Safety Telecommunications Council Unmanned Aircraft Systems and Robotics Working Group (2017) *Guidelines for Creating an Unmanned Aircraft System (UAS) Program*. Available at http://www.npstc.org/download.jsp?tableId=37&column=217&id=3901&file=Guidelines_for_Creating_UAS_Program_vs2_170418.pdf

[56] ANSI Unmanned Aircraft Systems Standardization Collaborative (2018) *Standardization Roadmap for Unmanned Aircraft Systems, Version 1.0*. Available at https://www.surveymonkey.com/r/TJTGZS9

[57] National Council on Public Safety UAS (2019) UAS Resources. Available at http://publicsafetyuas.org/#resources

[58] Criminal Justice and Health Collaboration Project Working Group, IJIS Institute, and Urban Institute (2013) Opportunities for Information Sharing to Enhance Health and Public Safety Outcomes: A Report by the Criminal Justice and Health Collaboration Project. Available at http://www.urban.org/publications/412788.html

[59] National Telecommunications and Information Administration (2017) Notice of Funding Opportunity State and Local Implementation Grant Program (SLIGP) 2.0. Available at https://www.ntia.doc.gov/nofo-sligp-20-09272017

[60] U.S. Department of Homeland Security (2016) VQiPS - Policy Considerations for the Use of Video in Public Safety. Available at https://www.dhs.gov/publication/vqips-policy-considerations-use-video-public-safety

[61] U.S. Department of Homeland Security (2018) Fiscal Year 2019 SAFECOM Guidance on Emergency Communications Grants. Available at https://www.dhs.gov/publication/funding-documents

[62] U.S. Department of Transportation National 911 Program (2016) Next Generation 911 Procurement Guidance. Available at https://www.911.gov/project_nextgeneration911procurementguidance.html

[63] IJIS Institute Public Safety Technical Standards Committee (2017) *CAD-to-CAD Data Sharing: A Review of Recommended Standards.* Available at https://cdn.ymaws.com/www.ijis.org/resource/collection/93F7DF36-8973-4B78-A190-0E786D87F74F/ijis_wp_IPSTC_CAD-to-CAD_Data_Sharing_-_Standards_20170317.pdf

[64] U.S. Department of Health and Human Services Office of the National Coordinator for Health IT (2019) *2019 Interoperability Standards Advisory*. Available at https://www.healthit.gov/isa/sites/isa/files/inline-files/2019ISAReferenceEdition.pdf

[65] U.S. Department of Transportation National 911 Program (2016) *Next Generation 911 Interstate Playbook, Chapter 1*. Available at https://www.911.gov/project_nextgeneration911interstateplaybook.html

[66] IJIS Institute (2016) *Information Sharing and Safeguarding (IS&S) Playbook, Version 2.* Available at http://standardscoordination.org/iss-playbook

[67] Open Knowledge International (2010) *Open Data Handbook*. Available at https://opendatahandbook.org/guide/en/

[68] Drees L, Castro D (2014) *State Open Data Policies and Portals*. Available at https://www.datainnovation.org/2014/08/state-open-data-policies-and-portals

[69] Dodds L (2016) *How to write a good open data policy* (Open Data Institute). Available at https://theodi.org/article/how-to-write-a-good-open-data-policy

[70] Civic Analytics Network (2018) *Eight Guidelines for Open Data*. Available at https://datasmart.ash.harvard.edu/news/article/eight-guidelines-open-data

[71] Future of Privacy Forum (2018) City of Seattle Open Data Risk Assessment. Available at https://fpf.org/wp-content/uploads/2018/01/FPF-Open-Data-Risk-Assessment-for-City-of-Seattle.pdf

[72] U.S. National Academy of Medicine (2018) *Procuring Interoperability: Achieving High-Quality, Connected, and Person-Centered Care.* Available at https://nam.edu/procuring-interoperability-achieving-high-quality-connected-and-person-centered-care

[73] National Information Sharing Consortium (2015) Virtual USA. Available at https://www.nisconsortium.org/nisc-activities/virtual-usa-2/

[74] National Information Sharing Consortium (2015) *Virtual USA Essential Elements of Information Publication Guidance, v1.0*. Available at

https://www.nisconsortium.org/portal/vusainfprod/NISC_EEI_Publication_Guidance_1.0.pdf

[75] National Information Sharing Consortium (2018) *Virtual USA National Information Sharing Agreement, v2.0*. Available at https://www.nisconsortium.org/portal/resources/

[76] Silicon Valley Regional Data Trust (2017) About Us. Available at http://www.svrdt.org/about-svrdt/

[77] U.S. Department of Homeland Security (2019) Infrastructure Protection Gateway. Available at https://www.dhs.gov/cisa/ip-gateway

[78] Fairfax County Department of Information Technology (2018) NCRnet. Available at https://ncrnet.us/ncrnet

[79] Rezaei R, Chiew TK, Lee SP, Aliee ZS (2014) Interoperability evaluation models: A systematic review. *Computers in Industry* 65(1):1–23. https://doi.org/10.1016/j.compind.2013.09.001

[80] National Public Safety Telecommunications Council EMS Working Group (2013) *EMS Broadband Application List for FirstNet PSAC.* Available at http://www.npstc.org/download.jsp?tableId=37&column=217&id=2885&file=EMS_App_List_110413F.pdf

[81] National Public Safety Telecommunications Council Public Safety Internet of Things Working Group (2019) *Public Safety Internet of Things (IoT) Use Case Report and Assessment Attributes*. Available at http://npstc.org/download.jsp?tableId=37&column=217&id=4195&file=NPSTC_PSIoT_Use_Cases_Report_190616.pdf

[82] National Public Safety Telecommunications Council Common Channel Naming Working Group (2018) Mission Critical Push to Talk: Considerations for Interoperability Talkgroup Naming and Management. Available at http://www.npstc.org/download.jsp?tableId=37&column=217&id=4172&file=NPSTC_MCPTT_IO_TG_Naming_181214.pdf

[83] U.S. Department of Homeland Security (2018) 2018 SAFECOM Nationwide Survey Results. Available at https://www.dhs.gov/publication/sns

[84] Middle Class Tax Relief and Job Creation Act of 2012, Public Law Number 112–96, 126 Stat. 212 Available at https://www.congress.gov/112/plaws/publ96/PLAW-112publ96.pdf

[85] International Telecommunications Union Radiocommunication Working Party 5D (2017) *Draft New Report ITU-R M.[IMT-2020.TECH PERF REQ]: Minimum requirements related to technical performance for IMT-2020 radio interface(s).* Available at https://www.itu.int/md/R15-SG05-C-0040/en

[86] Consumer Reports (2017) *The Digital Standard*. Available at https://www.thedigitalstandard.org/

[87] Brennan Center for Justice (2016) *Collection of state and local policies on retention and release of police body-worn camera video data*. Available at https://www.brennancenter.org/sites/default/files/Retention_and_Release.pdf

[88] U.S. Federal Emergency Management Agency (2017) *National Incident Management System Guideline for Mutual Aid*. Available at https://www.fema.gov/media-library/assets/documents/151291

Appendix A: Example use cases with a focus on data sharing policy considerations

The following scenarios describe events where first responders from multiple agencies work together to respond to an incident. These use cases focus on the data elements that the agencies could share and the policies supporting their collaboration. In the first use case, a common incident, a building fire requiring a response from two adjacent fire departments and an EMS agency, depicts data exchanges that are largely within the realm of existing technical capabilities, with relatively straightforward data sharing policies that could reasonably be implemented today. The second use case describes a much more complex scenario, involving primary and extended agencies and organizations, responding to a significant natural hazard affecting a large geographical area. This use case envisions the capabilities that could be utilized with more technically sophisticated and standardized data sharing systems and federated access control policies across the public safety community and adjacent systems. The purpose of the more complex use case is to demonstrate the potential value of a coordinated public safety-wide technical and policy architecture that could be accomplished through coordinated technical standardization and policy development. Note that these use cases are meant to provide a high-level summary of incidents that would, in reality, contain much more complexity and additional actions. We focus here on key actions that have direct implications for real-time incident data sharing interoperability.

A.1. Use case 1: Multi-agency response to a fire in a high-rise apartment building

Scenario. A fire breaks out at 6 p.m. on a weekday in a kitchen on the seventh floor of a 10-story apartment building in Riverside[22], a city within Marion County. The building fire alarm activates, which automatically alerts the Riverside Fire Department (RFD). Residents begin to evacuate and the nearest Riverside Public Safety Answering Point (PSAP) is automatically alerted. Due to the hazard of the high occupancy of the apartment building, RFD has an automatic aid policy for this location, and the communications center personnel immediately dispatch several units from RFD as well as the Marion County Fire Department (MCFD) and Riverside EMS (REMS). En route to the incident, the incident commander (IC) reviews the pre-planning documents for the apartment building[23] and sees that there is a mobility-impaired resident in unit #501. EMS personnel each have a tablet device containing a HIPAA-certified medical record portal which allows them to search for individuals based on

[22] Names and locations in this use case do not refer to actual localities, people, or agencies.

[23] Pre-planning documents could be provided in a platform that includes a digital voice assistant which reads the highlights of the plan aloud and can answer spoken questions about the plan so that responders can drive to the incident while reviewing the information safely.

name, birth date, and other personal data to quickly access their personal health information at the scene.

Incident Data Sharing. En route to the incident, the IC uses a tablet to create an incident in the situational awareness app. The app recognizes the IC's credentials and automatically queries the RFD's dispatch server for information about active incidents assigned to the IC's unit. The dispatch server returns the information about the incident to the situational awareness app, and automatically designates RFD as the lead agency and adds the assigned MCFD and REMS units as supporting agencies to the incident; this automatically assigns incident data access privileges to the corresponding MCFD and REMS personnel. On the tablet display, the situational awareness app populates a dashboard with the locations and profiles of all responding RFD, MCFD, and REMS responders, and a map indicating the real-time location of all responding unit vehicles. The IC can add a map layer showing the locations and status of nearby fire departments and EMS agencies to quickly request additional support if needed. The map also includes a layer (which all first responders at the incident can view) showing the locations of all nearby water hydrants and how they are connected to the water mains; the firefighters assigned to establishing connections to the fire hydrants refer to this map on the tablet in their vehicle prior to arrival at the scene. The situational awareness app also populates a list of available resources provided by the building: live surveillance camera feeds, building maps, and a list of residents and staff. When the RFD unit arrives on the scene, the IC establishes the command post in the building parking lot, including a large display screen for the situational awareness dashboard.

In the 4 minutes between the triggering of the fire alarm and the arrival of the first fire truck, many residents have evacuated the building and are gathering in the parking lot. Communications personnel at the PSAP continuously synthesize information about the fire collected from 911 callers (including text messages and videos) and social media and add relevant data to the incident dashboard through the situational awareness app. The primary search team enters the building and two firefighters are assigned to locate the mobility-impaired resident. Two firefighters are assigned to locate and shut off the utility controls. Two firefighters remain in the parking lot to identify the residents who have evacuated and any immediate medical needs. They find the resident who was in the apartment where the fire started, who tells the firefighters that they were not able to extinguish the fire before evacuating. One firefighter radios this information to the IC.

Inside the building, firefighters use heads-up displays on their self-contained breathing apparatus (SCBA) masks to navigate to their targets. For the mobility-impaired resident evacuation team, their SCBA mask displays show the resident's apartment number and a small map of the fifth floor and path arrow indicating the best route to the unit from the nearest stairwell. A similar mask display directs a different firefighter to the location of the utility shut-off controls. While the mobility-impaired evacuation team ascends the stairs, the IC views live footage from the fifth-floor security cameras on the situational awareness

dashboard. The IC notices that an individual in a wheelchair has entered the hallway and appears to be moving towards the elevator bank; they radio this information to the evacuation team and place a second marker on their mask map indicating the location of the elevators. When the evacuation team reaches the fifth floor, they navigate towards the elevators; they see the resident in the wheelchair in the hallway. After verbally confirming that he is the resident from unit #501 and that no one else in his apartment requires help evacuating, they carry him out of the building.

Meanwhile in the parking lot, one firefighter is recording which residents have already evacuated in a resident tracking app on their tablet. While en route to the incident, the IC also sent an emergency alert to all registered building residents and staff; recipients who were not in the building were asked to respond "SAFE", and those who do so are automatically marked as safe in the evacuation list. Residents who reply "HELP" are automatically connected to PSAP personnel to determine their needs. When the primary search team exits the building, they report "primary search all clear" to the IC, who records this information in the incident dashboard; the PSAP is alerted and transmits a "primary all clear" message to all responders.

The REMS units arrive and begin triaging residents and staff in the parking lot. Some residents experienced smoke inhalation while evacuating, and one experienced minor injuries from a fall while rushing down the stairs. In addition to interviewing patients as they are being treated, EMS personnel can look up patients in the EMS dashboard to determine if they have any specific risk factors, medication allergies, or conditions that require special treatment; the records in the EMS dashboard can also be used to call a patient's doctor or used as a reference if the patient becomes unable to communicate. One resident who experienced smoke inhalation has severe asthma and is not responding quickly enough to the treatment administered by EMS personnel, so they choose to transport the resident to the hospital in one of the three ambulances. Using the EMS dashboard, EMS personnel check if the nearest hospital can accept patients and send a notification to the receiving hospital containing a link to the patient's medical record in the portal and notes collected by the EMS personnel.

The MCFD unit arrives as the building evacuation is nearly complete, and the primary effort is shifting to putting out the fire. Firefighters inside the building are automatically transmitting footage from their body-worn thermal imaging cameras (TICs) to the incident dashboard. Based on TIC images on their heads-up displays, firefighters have reported hot areas in the vicinity of the apartment where the fire started. The IC instructs the MCFD to prepare to deploy their UAS while the remaining firefighters position the fire trucks for extinguishing the fire. The UAS is equipped with both a regular video camera and an infrared video camera. Shortly after the UAS powers on, both video streams appear on the situational awareness dashboard, each overlaid with map markers of key locations within the building. While the fire is being extinguished, the UAS team navigates the device to an area outside

the building near the unit where the fire started. They see a great deal of smoke coming out of many of the windows near the unit. The infrared video shows a heat map through the smoke, indicating that the fire has spread to some adjacent units. The IC radios this information to the fire truck commanders, who then instruct their teams in putting water on the burning areas. Eventually, the UAS infrared video shows no indication of active burning visible from outside. The IC requests to have the UAS navigate to the building's roof to check that no smoke is coming out of roof vents. Confirming this, the firefighting equipment retreats and the UAS enters the building to survey the interior. The IC determines that the fire has been extinguished.

There are still building residents who have not been reported safe in the parking lot or via the text message system; however, the surveillance camera video analytics in the situational awareness dashboard has not identified any individuals in the building hallways other than firefighters for over 15 minutes.

The IC sends a secondary search team into the building to conduct a full sweep of the building for any remaining occupants who have not yet been accounted for. During the search, the IC receives an alert on the situational awareness dashboard, from the body-worn accelerometers and heart rate sensors, indicating that firefighter Williams has fallen down and has an erratic heart rhythm on the eighth floor. The situational awareness app automatically sends an alert to firefighter Jacobs, who is near Williams, and firefighters Foster and Lopez, who are currently one floor above them; the alert instructs all three firefighters to navigate to Williams' location, and a small map appears on their mask to direct them. Jacobs finds Williams unconscious on the floor and begins carrying Williams toward the exit; Foster and Lopez arrive shortly thereafter and assist Foster in evacuating Williams from the building. An alert was also sent to the EMS personnel in the parking lot, and a real-time graph of Williams' heart rhythm appears on the EMS dashboard next to Williams' medical record summary; they note that Williams takes medication to treat high blood pressure. The EMS personnel prepare to administer an automatic external defibrillator (AED). When Williams is brought to the EMS personnel, they revive Williams with the AED shock, then transport Williams to the hospital. The remaining firefighters finish the secondary search and report "all clear," which the IC records in the dashboard.

Data Sharing Agreement. RFD, MCFD, and REMS frequently support each other with mutual aid. Over the past two years, the agencies organized a joint task force to acquire new data sharing devices and software, including:

- Body-worn devices for firefighters (heart rate sensors, accelerometers, ambient temperature and oxygen concentration sensors, SCBA status sensors, heads-up displays and TICs on SCBA masks);

- Indoor firefighter location tracking, based on body-worn location beacons and sensors deployed inside the building either before the incident (for selected buildings) or deployed by firefighters as they enter the building during an incident;
- A situational awareness dashboard which integrates all the data streams (including dispatch data), visually maps the locations of important features (e.g., responders, building hazards, water lines and hydrants, utility shut-offs), and generates alerts tailored to ICs and individual responders; and
- A medical record portal, built in collaboration with area hospitals, containing a summary of registered individuals' medical information (prescriptions, conditions, hospitalizations, basic vital information), and is linked to home and work/school addresses, emergency contacts, and healthcare providers.

Through a series of use case exercises, the agencies developed a data sharing framework which describes which responders need which data streams. For example, individual firefighter location data should be sent to all other firefighters (and displayed dynamically on heads-up mask displays) as well as to the IC dashboard, while firefighter biometric data should only be sent to ICs and authorized medical professionals (including EMS personnel and medically-trained firefighters). Once the data sharing framework was complete, the agencies drafted a data sharing agreement addressing each of the components described in Sec. 3.3:

- *Data Definitions.* The agreement lists all the types of data that may be available during incidents, and whether the data must conform to particular data exchange standards (including file formats and standard units of measure). In this use case, the data elements include:
    - Individual firefighter locations
    - Nearby hydrant locations and water line connections
    - Firefighter biometric data from wearable devices
    - Building floor plans
    - Building hazards information (water, electricity, and natural gas controls; hazardous materials; construction areas; etc.)
    - Location and status of nearby fire and EMS department resources
    - Streaming video from UAS (regular camera and infrared camera)
    - Streaming video from privately-owned surveillance cameras
    - Identities and medical record summaries of all building residents and staff
- *Data Management*: With multiple agencies and third parties contributing different data elements at different points throughout the life cycle of an incident, data management is an important issue. Depending on the manner in which the data are collected and distributed, the agencies may choose to delegate data management to a

central operation, or they may simply agree that whichever agency provides a particular data element is responsible for managing that data.

    - Management includes sending the data to a repository (such as a cloud server) where it can be accessed by applications, appending relevant metadata such as timestamps and device source, and ensuring the data are properly formatted. Agencies may also need to consider situations where both agencies are contributing their own streams of the same type of data.

- *Data Ownership.* For each data element, the data sharing agreement specifies which entity (an agency which is a party to the agreement, another government agency, the building owner, individual residents, etc.) has ownership, and whether any circumstances (such as sharing the data with other parties) affects data ownership.

    - The agencies define rules for retaining or sharing ownership of data generated before, during, and after the incident. For example, agencies may collaborate before the incident to populate the situational awareness dashboard with static information, such as the locations of building hazards, water mains, and other utilities. Some of these data may derive from other city agencies or private businesses, and are thus owned by third parties, whereas the agencies may claim sole or shared ownership of data they collectively generate specifically for incident response planning. They may choose to claim joint ownership of certain data elements, while other data elements are owned by whichever agency creates them. Some of the devices acquired by the agencies may involve a data storage and analytics solution managed by the product vendor, with the vendor retaining ownership of the data.

    - In the case of the medical record portal described in this use case, building residents agree to allow access to their medical information to RFD, MCFD, and REMS first responders through the terms of their lease agreement, or the terms of their employment in the case of staff. As protected health information, these data are owned by the individuals, and managed by their medical providers, hospitals, and the RFD, MCFD, and REMS in compliance with HIPAA regulations.

- *Data Access.* Based on the use case exercises, the RFD, MCFD, and REMS have determined rules for which entities have access to which data elements.

    - There are both legal and operational aspects to these decisions. For example, some firefighter biometric data may include protected health information, and therefore, may only be legally shared with specific authorized parties unless it is sufficiently anonymized or aggregated. Operationally, an individual may be authorized to receive information, but visualizing and generating alerts for all authorized recipients may not be desirable. For example, a low-level health

alert from an individual firefighter may not be useful information to share with all other firefighters, therefore it may only be made available to ICs.

    - In this use case, if the agencies have access to any data access control mechanisms that extend beyond the signatories of the data sharing agreement (i.e., a mechanism that would allow additional entities, such as law enforcement officers or utility operators, to be provided with data access through the situational awareness dashboard), they are described in detail.

- *Data Security Practices.* The agreement specifies physical and logical security procedures required by both agencies to participate in data sharing.
    - The agencies have agreed to certain cybersecurity practices for both stationary and mobile communication devices, such as installing anti-virus software, requiring two-factor authentication for mobile devices at least once per 24-hour period, and monthly security audits[24]. They also specify how physical access to IT infrastructure, including incident command posts, is controlled.
- *Data Integration.* The agencies map their data sharing requirements onto operational use cases. Use cases include both internal and external functions such as real-time incident data sharing associated with specific technologies (CAD, apps, video systems, etc.), records management systems, and bookkeeping. The agreement states whether each data element must conform to a particular data exchange standard.
    - This portion of the agreement documents both the level of integration exhibited by the technologies currently in use by the participating agencies and the interoperability expectations for technologies that are integrated into mutual aid operations in the future. For data sources outside the control of the participating agencies (e.g., private video camera systems not integrated into building pre-plans), the agreement describes how data sources that do not meet their standardization requirements can be integrated into their shared data environment (for example, using a translation tool). The requirements identified for future technologies provide documentation that the agencies can use when negotiating with vendors about the features and capabilities of new products.
- *Data Retention.* The agreement articulates whether each data element will only be shared during an incident or will be stored after the incident, for how long data will be stored, the way data are stored and protected from unauthorized access, and the procedure for deleting the data.

[24] For example, following the NIST Framework for Improving Critical Infrastructure Cybersecurity, https://www.nist.gov/cyberframework.

    - Streaming data with no long-term storage has the benefit of avoiding storage costs and security risks and associated legal liabilities. However, some data may need to be retained (e.g., to create forensic records) or may be useful for research and training purposes. In some cases, there may also be a legal requirement to retain data (e.g., video from body-worn cameras [87]). Agencies should consider that data may be stored temporarily, even if it is not explicitly stored in a long-term repository (e.g., browser caching, server transmission), which may still carry legal and security liabilities. Agencies may wish to establish procedures for verifying how long data are stored and that data have been deleted.

- *Data Redaction.* The agreement articulates whether any sensitive data requires redaction for post-incident storage or further dissemination.
    - Some of the data included in the agreement may be sensitive, meaning its disclosure to unauthorized parties could result in legal consequences or operational risks. If any sensitive data are stored or retained after the incident, the agreement specifies how the data will be redacted so that they can be shared with third parties (e.g., for research purposes or to fulfill public records requests), and whether it is necessary to retain an unredacted copy (e.g., for forensic purposes).
- *Data Policy Consistency.* The agreement articulates whether any pre-existing agency policies affect how they can share the data elements in the agreement.
    - If there are differences between the agencies in such policies, the agreement states how these differences are dealt with. For example, if the agencies had pre-existing data security policies, they may describe how the policies articulated in the data sharing agreement are more stringent, and therefore supersede the pre-existing agency policies. If inconsistencies are identified, agencies may choose to update or eliminate outdated policies to align with the policies in the inter-agency agreement. Agencies also discuss procedures for applying software updates in coordination to prevent interoperability problems due to version inconsistencies.

The agreement also addresses legal indemnification in the event that either agency, or a third party, fails to handle any data described in the agreement according to the terms of the agreement. For data elements which are owned or managed by third party vendors, the agreement specifies how the vendor's data security, retention, and redaction procedures meet the relevant policy requirements. In acquiring the devices and software packages implementing the Data Definitions in their data sharing agreement, RFD, MCFD, and REMS negotiated with their vendors to require that the products met their technical requirements and policy needs.

After numerous tabletop exercises, trainings, and piecemeal implementations, the technologies are now woven into the everyday operations of all three agencies. When the agencies meet at an incident, responders can simply log on to the situational awareness app and watch the data begin populating the incident dashboard. When the incident is complete, any data tagged for retention is automatically stored on the servers of the agency that owns it.

Use Case 1: Key Takeaways.

- The agencies collaboratively developed a list of shared goals for data sharing, which informed the development of a detailed data sharing agreement and technology procurement decisions.
- Data sharing decisions depended on a combination of operational requirements (who needs what information), legal constraints, and security principles.
- The data sharing described in this use case requires nuanced, flexible controls on data access and data sources that conform to standards that are understood by the situational awareness dashboard.

A.2. Use Case 2: Streamlined mutual aid across jurisdictions and disciplines for major incident response

Scenario. In response to a large earthquake, the governor of a state declares a state of emergency and, through the Emergency Management Assistance Compact (EMAC)[25], requests support from neighboring states. This use case assumes that a *data sharing framework* development process similar to that described in the first use case was carried out at a national scale. The steering committee which led the process used the NIMS Guidelines for Mutual Aid [88] and existing mutual aid agreements as a foundation to build a software program that leverages an access control model similar to the Trustmark Framework. The final outcome of this process was the creation of an **Emergency Incident Data Hub (EIDH)**, which serves all agencies which participate in EMAC.

Incident Data Sharing. The earthquake has caused varying amounts of damage across a multi-state region. In general, the responding agencies do not have direct experience working together in mutual aid situations. Rather, in response to the governor's declaration, a predetermined authority in each state, such as the Director of the State Department of Emergency Management, activates the state's EIDH which serves as a platform for agencies to discover informational, physical, and personnel resources of all participating agencies[26]. Due to the official declaration of a state of emergency, FEMA and other relevant federal

[25] EMAC, created by U.S. Public Law 104-321, provides a legal foundation for coordinated mutual aid requests across state boundaries, https://www.emacweb.org.

[26] If the governor had not declared a state of emergency, as required for the activation of EMAC, the state authority can delegate another level of government to activate the EIDH; e.g. for an incident affecting multiple counties, the county executive could authorize activation of the EIDH.

agencies are automatically included in the EIDH incident, and the incident is assigned a FEMA mission number. Requests for inter-state resources are entered into the EIDH and must be authorized by a FEMA authority.

By default, the Department of Emergency Management of the state which initiated the activation of the EIDH is considered the lead agency (this can be delegated by the department to another agency if desired). The lead agency sends out requests to agencies to enter the EIDH, either by manually selecting agencies or by setting criteria (e.g., EMS departments within 100 miles) and allowing the EIDH to automatically alert agencies meeting the criteria. Agencies who did not receive direct requests to join can also enter the EIDH. Other agencies can submit requests to the lead agency asking that an agency be invited or inter-state resources requested; however, only the lead agency can execute these actions within the EIDH.

Each agency has a designated **Agency Data Manager (ADM)**, which can be a single individual or a team[27]. ADMs ensure that their agency data resources are linked to the EIDH throughout the incident and select the appropriate status for their agency (fully operational, partially operational, requesting support, offering support, etc.). If the agency status is not changed or re-confirmed within a certain time interval, it is automatically set to "unknown." All agency data are classified by categories (e.g., live video, floor plans, personnel, etc.), and these categories are automatically applied when the ADM links their agency data resources to the EIDH. A pre-defined hierarchy of back-up ADMs at each agency ensures that every agency will maintain an active ADM throughout the incident if a primary ADM cannot carry out their role.

Any first responder with an authenticated credential issued by their home agency can access the EIDH. The EIDH can be used as either a web interface or a mobile application. First responders log in using a physical token and entering their username and password (i.e., two-factor authentication). The EIDH authenticates users' credentials by exchanging encoded policy assertions with the responder's home agency. The EIDH authenticates that the agency's policy assertions are valid, and then accepts the agency's assertions about the specific data access permissions of the individual logging in. In addition to basic information such as rank and role, the agency may assert that an individual has specific trainings and certifications, which the EIDH policy program can interpret to grant access to particular types of data. For example, an agency may assert that an individual has federally accredited certification to access protected health information. If another agency provides data containing such information to the EIDH and makes the data accessible to all policy-conformant responders, the certified individual will automatically be granted access to the data, while responders without this certification will not.

[27] Due to the complexity of the ADM role, some decision-making could be supplemented with artificial intelligence built into the EIDH system. Such functionality would need to be agreed to by all participating agencies and extensively tested before use during a major incident.

By default, all authenticated EIDH users affiliated with public safety agencies can view a set of basic information, referred to as "baseline incident data," about each participating public safety agency:

- Agency name
- Agency location(s) (headquarters, field command posts, and/or temporary sites, as appropriate)
- Contact information of agency operations leaders (direct phone number and email address for at least two individuals per agency; distinct from the agency's public information office)
- Agency status and the time when status was last verified
- Number of first responders under agency's command, separated by roles
- Identity of the lead agency

Within the EIDH, the baseline data are keyword-searchable (within the domain of data to which the individual has access) and displayed in various layers on a map interface. All users can set personal alerts for information, e.g. an alert that a particular fire department status changes from partially operational to fully operational. By default, each responder has access to all data provided by their own agency, unless asserted otherwise by their agency during the credential authentication step.

The EIDH login also performs a single sign-on, linking the individual's profile to other EIDH-verified applications on their device (e.g., incident messaging, video streaming, and situational awareness apps). This links the EIDH to these external apps, allowing the agency's preferred apps to utilize any EIDH data to which the individual has access. **Data from the EIDH are formatted according to specific open data exchange standards, allowing any app which understands these specifications to use EIDH data and exchange EIDH data with each other.** The formats of data ingested by the apps are standardized; however, an app may produce analytics or alerts based on EIDH data in proprietary formats that can only be accessed by users of that particular app.

The ADMs are able to adjust data access privileges of all EIDH users. Within the EIDH, ADMs can select whole agencies, role categories, or specific individuals to be permitted access to more detailed data generated by their agency, and to reduce agencies, role categories, or individuals to the baseline access level, or to block access to even the baseline data (a backstop measure in the event of misuse or suspected security breaches). These access adjustments are performed through the ADM's administrator profile in the EIDH, which visualizes the data access privileges of individuals, role categories, and agencies in a flexible and searchable manner. For example, at the outset of an incident, an agency ADM may choose to grant access to the real-time locations of their agency's vehicles to EIDH users designated as field commanders or agency chiefs.

Individuals can also request access to more comprehensive data beyond the baseline incident data. All data in EIDH are discoverable to public safety users, so users can see data that exist in the system, but to which they do not have access[28].

> **Mini-Scenario: Ad hoc data request.** During the earthquake response, the chief of a small rural fire department has dispatched their units to a suburban shopping mall outside their jurisdiction which experienced structural damage. The complex was evacuated, but some victims at the scene report that they have not located everyone in their party, and the chief determines that the exit of one of the bathrooms may have become inaccessible, trapping a few people inside. The chief sees on EIDH that the local police department has linked the mall's security camera system and floor plans to the EIDH. The chief requests access to the live video data, and the ADM at the police department confirms that the fire department complies with EIDH video data policies, and that the unit is already at the scene. The police department ADM approves the fire chief's request and they access the camera system through a streaming video module in their situational awareness dashboard. Based on information from the victims, the chief determines which video cameras are likely near the blocked bathroom door and selects these cameras to display on the EIDH interface. The chief notices what appears to be rubble in the display from one of the cameras and plots an access route to reach the victims at that location. As the firefighters enter the mall and search for the victims, the chief watches their progress on the video displays. When the chief (or any user) accesses a video stream through the EIDH, the EIDH triggers the storage of the video feed that is viewed, beginning at the time they are accessed until the user clicks a "disconnect video" button on their EIDH interface; if the video system temporarily stores past video, the EIDH captures any cached video prior to the time when the user accessed the stream and tags this portion of the stored video file as "pre-view."

Second responders, non-public safety entities who may be involved in disaster response (e.g., transportation agencies, utility operators, scientific researchers, school administrators), can also pre-enroll in the EIDH system (i.e., in advance of an actual incident). Once such a support entity has linked its internal credential and data access permission system to the EIDH policy program, their personnel can log into the EIDH and place a request for data access in the same manner as public safety users do[29]. Data in EIDH are not discoverable to

[28] Data are discoverable according to metadata attached to the data. For example, video data can include metadata indicating the data type (video), the location of the camera, the identity of the operator, and other information. Some metadata may be considered too sensitive to be visible to all public safety users. Data providers can adjust the viewing privileges of metadata categories to mitigate the risk of information leak from metadata. If no metadata categories are visible to a given user, then that data source is effectively not discoverable to them.

[29] Second responders enrolling in EIDH are required to take training on appropriate use of the EIDH and sign an agreement stating that they will not misuse the EIDH during an incident, for example by making data requests that are not necessary or do not contribute to incident response.

second responder users by default; rather, public safety agencies must opt in each type of data they provide if they wish to make it discoverable to second responder users. If a second responder user desires access to data that are not visible to them in EIDH, they must place a request with the appropriate ADM(s). Each second responder entity also has a designated ADM performing the same duties as the public safety ADMs. If a second responder entity is considered central to the overall incident response, the lead agency can choose to elevate that entity to the data access level of public safety users. For example, in a major earthquake incident response, the lead agency may determine that transportation authorities must be involved in all aspects of the response and chooses to allow public safety-level EIDH access to all transportation agency users.

By default, second responder users are given access to only a subset of the baseline incident data describing participating public safety agencies:

- Agency name
- Agency location(s) (headquarters, field command posts, and/or temporary sites, as appropriate)
- Contact information of agency operations leaders (direct phone number and email address for at least two individuals per agency; distinct from the agency's public information office)
- Identity of the lead agency

Second responder users can link their data resources to the EIDH in the same manner as public safety users, and their ADMs can likewise grant and restrict access to other EIDH users. All data provided to the EIDH by second responder entities are discoverable to public safety users. As an example of how data from secondary responders can contribute to the incident response, the fire chief leading the evacuation/rescue operation at the suburban mall wants to ensure that a power outage does not disrupt the surveillance video feed. They see that the mall's utility operator is logged into the EIDH, and available data resources include electrical system status. The chief requests access to the system status. The utility ADM grants access and the fire chief sees that the mall's status is "running on back-up generator power." Since the generators may not be able to power the entire complex for very long, the chief requests access to the locations of emergency generators, and sends a message to the utility contact asking which generator(s) specifically provide power to the surveillance camera system, any instructions on how to physically access the generators (presuming they are in a secure location), and requesting permission to refuel the generators as necessary.

If a second responder entity is not pre-enrolled in the EIDH credentialing and access permission system but wishes to provide incident-relevant data or believes they have a legitimate need for incident data, they may submit an ad hoc request for access. The ad hoc access request form asks an applicant to provide the entity's name and contact information, which data categories they can provide or to which they would like access (e.g., a digital elevation map for a chemical plant), any specifications regarding data formats, a brief

explanation of why they require EIDH access, and a tag for the level of urgency they associate with their request. The submission is routed to the lead agency's ADM, and the ADM can choose to respond to such requests at their discretion. Depending on the assigned urgency level, if the ADM does not respond to the request within a certain time limit, the EIDH will automatically send reminders and/or send the request to additional agency leaders; the requesting entity can track the progress of their request in the EIDH (external view). If the ADM believes the request has merit, they will contact the applicant (most likely over the phone) to discuss any concerns (e.g., security risks) and technical issues (e.g., the entity's data does not conform to the same data standards as are used by the EIDH)[30]. If the request is approved, the second responder entity may be given temporary access to certain data categories and may link their data resources to the EIDH[31].

All actions taken within the EIDH (logins, data resource linkages, data requests, and data searches), whether successful or not, are logged with a timestamp and the identities of the users involved. As agencies scale down their involvement, individuals no longer assigned to the incident log out of the EIDH; when the whole agency is no longer participating in the incident, an agency's ADM can suspend their agency's participation in the incident, which must be acknowledged by the lead agency before the departing agency is removed from the EIDH incident. When the lead agency determines that continuous inter-jurisdictional coordinated operations are no longer necessary, they close the incident in the EIDH, and once the action is confirmed by a FEMA authority, all agencies still participating in the incident are removed from the EIDH incident.

At this point, the lead agency initiates deactivation of the EIDH. The encoded policy rules associated with each data category automatically enforce procedures for post-incident data retention. In most cases, data ownership will be applied to the agency which provided the data to the EIDH. The EIDH generates a summary for each agency describing the data resources provided by their agency, which agencies accessed those resources, which resources their personnel accessed from other agencies, and what data products were retained for them in the EIDH following the incident. Among other things, this allows the agency to determine whether they need post-incident records of data products that were not automatically generated by the EIDH (e.g., images collected by another agency during an operation in which their personnel assisted). The EIDH also generates a summary report of the entire incident, listing the participating agencies and second responder entities, the number and type of data requests, and a timeline of operations. A copy of the full incident

[30] The EIDH is designed to avoid the need for such negotiations through built-in data translation capabilities and a federated identity management and access control model. However, recognizing the possibility that these tools may not be able to address every possible complication, it is always possible to contact individuals directly.

[31] Depending on the incident circumstances (severe time constraints, degraded network conditions, etc.), the lead agency's ADM may decide that the need for incident information outweighs the potential risks of less restricted access to the EIDH for some or all types of second responder users who are not pre-enrolled. They may then choose to lift the approval requirement for assigning EIDH privileges to such users.

summary report is produced for all participating public safety agencies, which they will use for filing reimbursement costs with FEMA (among other purposes).

Once the EIDH incident is deactivated, ADMs can login to access retained incident data, such as video and image files and message threads, and transfer the files to their own data repositories. Once an ADM has completed this transition, they confirm in the EIDH that they have accepted ownership of the data and the data can be permanently deleted from the EIDH after a predetermined retention period.

Use Case 2: Key Takeaways.

- The lead agency initiated an incident within the EIDH, allowing all first and second responders to view other responding agencies and assets and request information as necessary.
- Built-in policies determined what information different users have access to by default or upon request and automatically applied data retention policies following the incident.
- ADMs played a central role by integrating their agency's resources with the EIDH and responding to data requests as necessary.
- Detailed EIDH logs provided agencies with records of data use by their personnel and other responders.

Appendix B: Additional Public Safety Data Exchange Standards

Sec. 3.1.1 discussed the data exchange standards EDXL, NIEM, EIDD, and NFPA 950 in some detail. The following list includes additional standards related to public safety data exchange. This is not an exhaustive list but is intended to provide a sense of the variety of standards that have been developed for public safety data sharing.

APCO/CSAA ANS 2.101.2-2014 Alarm Monitoring Company to Public Safety Answering Point (PSAP) Computer-Aided Dispatch (CAD) Automated Secure Alarm Protocol (ASAP)[32]. Protocols for automating communication between alarm monitoring central stations (i.e., private alarm systems), PSAPs, and CAD systems.

APCO ANS 1.111.2-2018: Public Safety Communications Common Disposition Codes for Data Exchange[33]. Enables disparate PSAPs and other authorized agencies to share incident disposition information.

IEEE 1512: Common Incident Management Message Sets for Use by Emergency Management Centers[34]. A set of messaging standards for Traffic Incident Management[35] and Hazardous Material Incident Management[36].

IETF RFC 7852: Additional Data related to an Emergency Call[37]. An XML standard defining formats of data exchanged during a call to a PSAP.

NENA-STA-012.2-2017: NG9-1-1 Additional Data[38]. Includes information about an emergency call, call location, and the caller. Based on EIDD and builds on IETF RFC 7852 (above).

NFPA 1221: Installation, Maintenance, and Use of Emergency Services Communications Systems[39]. The standard includes many requirements for CAD data sharing, including access control measures (§10.3), interoperability of alarms between CAD systems (§10.4), CAD data retention (§10.9.2), data retention of mobile data computers (§10.11.5.5), and cybersecurity (§13.1.2).

[32] https://www.apcointl.org/resources/interoperability/asap/asap-to-psap-background.html
[33] https://www.apcointl.org/download/apco_ans_1-111-2-2018-disposition-codes/?wpdmdl=5997
[34] https://standards.ieee.org/standard/1512-2006.html
[35] https://standards.ieee.org/findstds/standard/1512.1-2006.html
[36] https://standards.ieee.org/findstds/standard/1512.3-2006.html
[37] https://tools.ietf.org/html/rfc7852
[38] https://www.nena.org/page/NG911_AdditionalData
[39] https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=1221

NFPA 3000 (in progress): Standard for an Active Shooter/Hostile Event Response (ASHER) Program[40]. An explicitly cross-jurisdictional standard (§8.4.2) with many elements related to data sharing (§11.5).

[40] https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=3000