SAFECOM NCSWIC

Information Sharing Framework Task Force

Approach for Developing an Interoperable Information Sharing Framework

---

Version 1.7

Publication: August 2021

Cybersecurity and Infrastructure Security Agency

This Page Intentionally Left Blank

INFORMATION SHARING FRAMEWORK TASK FORCE MEMBERS

This project would not have been possible without the combined expertise and support from the members of the Information Sharing Framework Task Force (ISFTF). Their feedback throughout the development of this document has been invaluable. It has been a challenging assignment to provide guidance to practitioners that is operationally relevant yet specific enough that information technology staff can develop the necessary requirements to design and implement an interoperable system.

This report is not intended to replace valuable work that is ongoing by the Cybersecurity and Infrastructure Security Agency's (CISA) federal partners and various public safety associations, but rather complement those efforts by proposing an overarching interoperability framework that organizes the collective thinking on how these elements come together in an effective solution. We are indebted to the following Task Force members for collaborating on such an important effort that will help to ultimately achieve an interoperable public safety ecosystem.

ISFTF Co-Chairs	TITLE	ORGANIZATION	CONTACT INFORMATION
Fitzgerald, Paul	Sheriff	Story County Iowa	pfitzgerald@storycountyiowa.gov
Lewin, Jonathan	Chief (Retired), Bureau of Technical Services, *Former SAFECOM Member*	Chicago Police Department	chicagopolice.org
ISFTF	**TITLE**	**ORGANIZATION**	**CONTACT INFORMATION**
Contestabile, John	Director Public Safety Solutions	Skyline Technologies Solutions	jcontestabile@skyline.net
Dew, Rob	Senior Technologist	Cybersecurity & Infrastructure Security Agency, Emergency Communications Division	robert.dew@cisa.dhs.gov
Galvin, Joe	Program Manager Strategy, Performance, & Resources	Cybersecurity & Infrastructure Security Agency, Emergency Communications Division	joseph.galvin@cisa.dhs.gov
Jacobson, Michael	Information Sharing Specialist	SAFECOM	mjacobson@search.org
Jurrens, Karla	Deputy Statewide Interoperability Coordinator	Texas Dept. of Public Safety	karla.jurrens@dps.texas.gov
Magnussen, Walt	Director	TAMU Internet2 Technology Evaluation Center	w-magnussen@tamu.edu
Maiers, Chris	Statewide Interoperability Coordinator	Iowa Dept. of Public Safety	maiers@dps.state.ia.us
Sasser, Charlie	Senior Officer	SAFECOM & National Association of State Technology Directors	charlie.sasser@gta.ga.gov
Stoddard, Brad	Statewide Interoperability Coordinator	Michigan Dept. of Technology, Management & Budget	stoddardb@michigan.gov
VandenHeuvel, Jared	Program Coordinator	Texas Dept. of Public Safety	jared.vandenheuvel@dps.texas.gov
Waldner, Mike	Project Manager	Bureau of Information & Telecommunications, State of South Dakota	mike.waldner@state.sd.us

EXECUTIVE SUMMARY

The desire to improve the efficiency and effectiveness of communications and information sharing for our Nation's public safety agencies has led to an ever-growing market of platforms and solutions that do not always address operational needs. As a result, agencies continue to invest in new products and technologies to improve their public safety communications ecosystems. However, many of these new products and technologies force trade-offs among interoperability, flexibility, security and sustainability, which impacts time to value for any agency. The solutions often attempt to position their product as the central predominant technology without due consideration to the long-term impact to the end users' mission environments and their ongoing interoperability requirements. Typically, the public safety agencies must manage a multitude of platforms and systems that don't interoperate and burden the agency with technical complexity and incomplete situational awareness.

Acknowledging the need to support our public safety agencies, SAFECOM and the National Council of Statewide Interoperability Coordinators (NCSWIC) in partnership with the Cybersecurity and Infrastructure Security Agency (CISA) have established the Information Sharing Framework Task Force (ISFTF) comprised of information technology (IT) and public safety communications subject matter experts from public safety agencies across the country.

CISA is engaging with the ISFTF to develop an Information Sharing Framework (ISF) to ensure the effectiveness of new products and technologies as agencies transition to mobile and fully interconnected environments. Making data interoperable and enabling information sharing across platforms is a requirement that spans beyond technical and traditional organizational boundaries. First responders should be able to discover, access, and consume any relevant information on a need-to-know basis, regardless of jurisdiction, affiliation, or location.

The intended audience for this ISF document includes Statewide Interoperability Coordinators (SWICs) and other state and local level public safety communications personnel working with land mobile radio (LMR), cellular broadband, 911, public alerts, warnings, and notifications (AWN) systems, and any personnel directly involved in acquisition, management, and oversight of public safety systems. The document is organized as follows: [*Note: use "CTRL + click" on the bold title of a section or Appendix to navigate to that area of the document*]

- **Section 1 - Introduction** provides the role and objectives of the Information Sharing Framework (ISF)
- **Section 2 - Document Organization** provides a description of each section of this document, and where appropriate the intended audience for that section
- **Section 3 - Background** provides an overview of the phased approach and an overview of baseline work accomplished to date
- **Section 4 - Information Sharing Framework** provides a high-level overview of the approach for developing and implementing an information sharing framework
- **Section 5 - Summary** provides a high-level summary of the information found within the body of this document
- **Appendix A - Baseline Technological Assessment** presents the results of a baseline technological assessment of emerging technologies and best practices and is ***intended for those interested in a deeper understanding of the technological aspects relevant to achieving interoperability***.
- **Appendix B - Use Cases** presents information on a sampling of representative use to help develop baseline requirements and is ***intended for both operational and technical personnel***.
- **Appendix C - Policy Considerations** provides a discussion regarding the policy considerations that should be considered in the implementation of the ISF. This appendix is ***intended for all public safety personnel with decision making roles and responsibilities.***

- **Appendix D - Functional and Physical Architecture Approach Overview** provides a more technical understanding of the interoperability needs of the end-user and the technology community and is ***intended for the public safety IT community.***

- **Appendix E - ISF Implementation Cycle** provides tools and resources to help guide each of the six (6) steps of the ISF Implementation Cycle. This appendix is ***intended for public safety personnel who have responsibilities for implementing interoperability programs (e.g., acquisition, training, CONOPS development, etc.).***

- **Appendix F - Acronym Lists** provides a list of acronyms and definitions used in this document as well as a list of common emergency communications acronyms.

The overarching goal of the ISF is to inform and guide the transition of operational capabilities to a common data exchange approach that a public safety entity can adopt and use efficiently. Many public safety organizations experience the same challenges and may benefit from this framework.

This approach must consider several dimensions of interoperability including common data structures and formats, common transport/messaging protocols, common search and information request service calls, and network and communications interconnectivity. The value proposition of the ISF for SWICs and other public safety personnel is to provide:

- An interoperable, operational architecture that can be customized to specific public safety use cases and that ensures alignment of people, processes, and technology prior to a major multi-agency, multi-jurisdiction event or investment;
- A roadmap to solving interoperability issues and gaps via architectural blueprints and governance that drives acquisition guidance and alignment with training, exercises and grants;
- A guidebook for public safety acquisition decisions for products and services ensuring that such acquisitions are interoperable, secure, resilient, and enable effective data management;
- A blueprint that informs state leadership of the complexities and needs for interoperability across multiple networks/functions (e.g., LMR, broadband, Next Generation 911 (NG911), Computer Aided Dispatch (CAD)/Record Management Systems (RMS), AWN, etc.) as well as political jurisdictions;
- A framework that incorporates information sharing best practices, guidance, and lessons learned; and
- A strategy for ISF evolution that can be expanded to include public safety IT personnel such as IT Service Unit Leaders (ITSL) and communications personnel such as the Communications Unit Leader (COML) as well as an ongoing dialogue and documentation of effective practices.

The ISF approach to addressing interoperability is based on a proven approach of defining interfaces and interoperability between enterprises. It includes several architectural views including:

- A *logical layered model* of data and information that can depict and demonstrate how disparate raw and processed data is transformed into useable information and shared;
- A *functional information exchange model* that depicts the major types of entities involved in public safety along with the typical function-based information exchanges that are required to happen among the entities in order for them to perform their mission(s) efficiently and effectively and that are enduring over time; and
- A *physical interface model* that incorporates the above two models and provides a more tangible description of how the public safety entities need to interface using multiple but related dimensions which include applications, services, devices, networks, and facilities.

The logical, 3-layered model (see Figure ES-1) presumes that existing legacy systems located in the *data layer* are not necessarily designed for sharing across platforms inside or outside the agency. They are more than likely stove-piped and closely-coupled to proprietary systems and applications. In addition, today's *presentation layer* tools are increasingly found in applications that reside on wireless smart devices. Thus, interoperability between these legacy data systems and the presentation of that data or information needed by emergency responders

must be addressed by an *integration layer* where the data is discovered, accessed, transported, processed, aggregated, manipulated, and analyzed into useful information. The resulting information should then be *transported/*delivered in a standard fashion to the presentation layer so that any public safety partner can consume the desired information in the application of their choice and improve their situational awareness. Additional information, including a description of the challenges associated with interoperability, can be found in the Phase 1 Interoperability Report located in the SAFECOM Governance Resources Publications Library at cisa.gov/publication/governance-documents

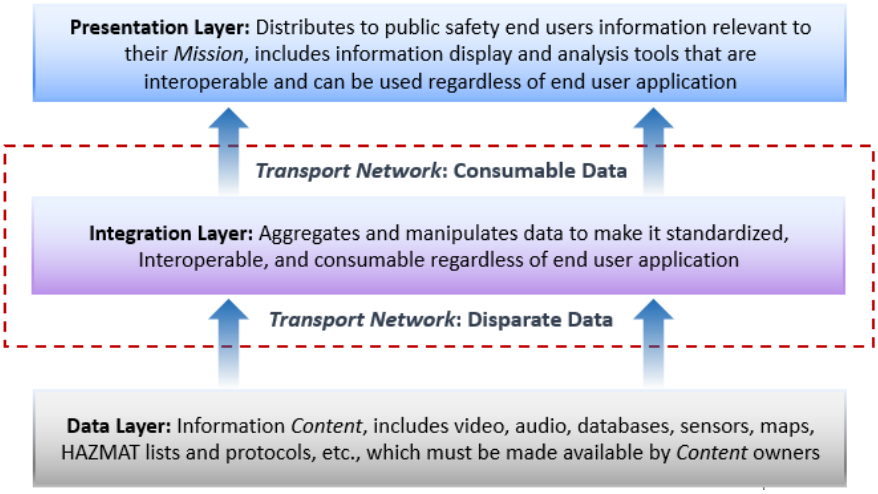


Figure ES-1: Conceptual Data-Information Model

The ISFTF recognizes that interoperability is a complex challenge beyond technology. The lack of interoperability is comprised of three dimensions that must align: *people, process, and technology* (see Figure ES-2). The people issues involve a lack of consensus across all the stakeholders on the need to share information (and in doing so, address the data interoperability issues). The process issues involve not having a protocol or other mechanisms to guide the necessary information sharing. And finally, even if there is agreement amongst the parties to share information, and there is a protocol and governance to guide the information sharing, there are technology issues and security considerations that must be addressed. Success will only occur when there is alignment across each of these aspects of the interoperability challenge. This complexity points to the need to approach this challenge using Enterprise of Enterprises (EoE) Architecture constructs. Data and information sharing success only occurs when the people involved jointly agree to share their data, establish processes to do so, and have a standard, technological approach that enables that agreement.

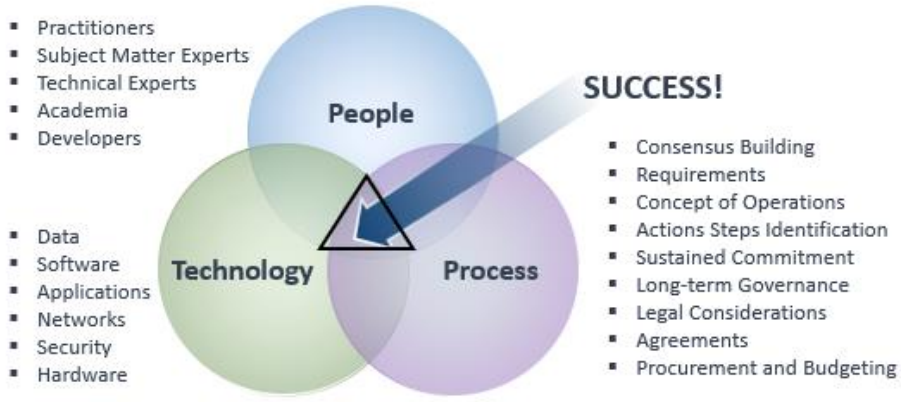


Figure ES-2: Interoperability Components

Given the scope of the Internet and the rapid increase of devices coming online in the Internet of Things (IoT), *discovery* and access to such a large amount of information poses significant challenges to avoid overwhelming end users with information beyond what is needed for the decision-making at hand. When additional information is added for the intended purpose of enhancing situational awareness, consideration must be given to ensuring that the right information is available at the right time to the right individual that is relevant to the current mission. In addition to enabling the exchange and transport of data and information between content owners (in the data layer) and end users (in the presentation layer), the integration layer needs to provide the *analytics* critical to ensuring that the information is timely, accurate, relevant, and targeted (see Figure ES-3).

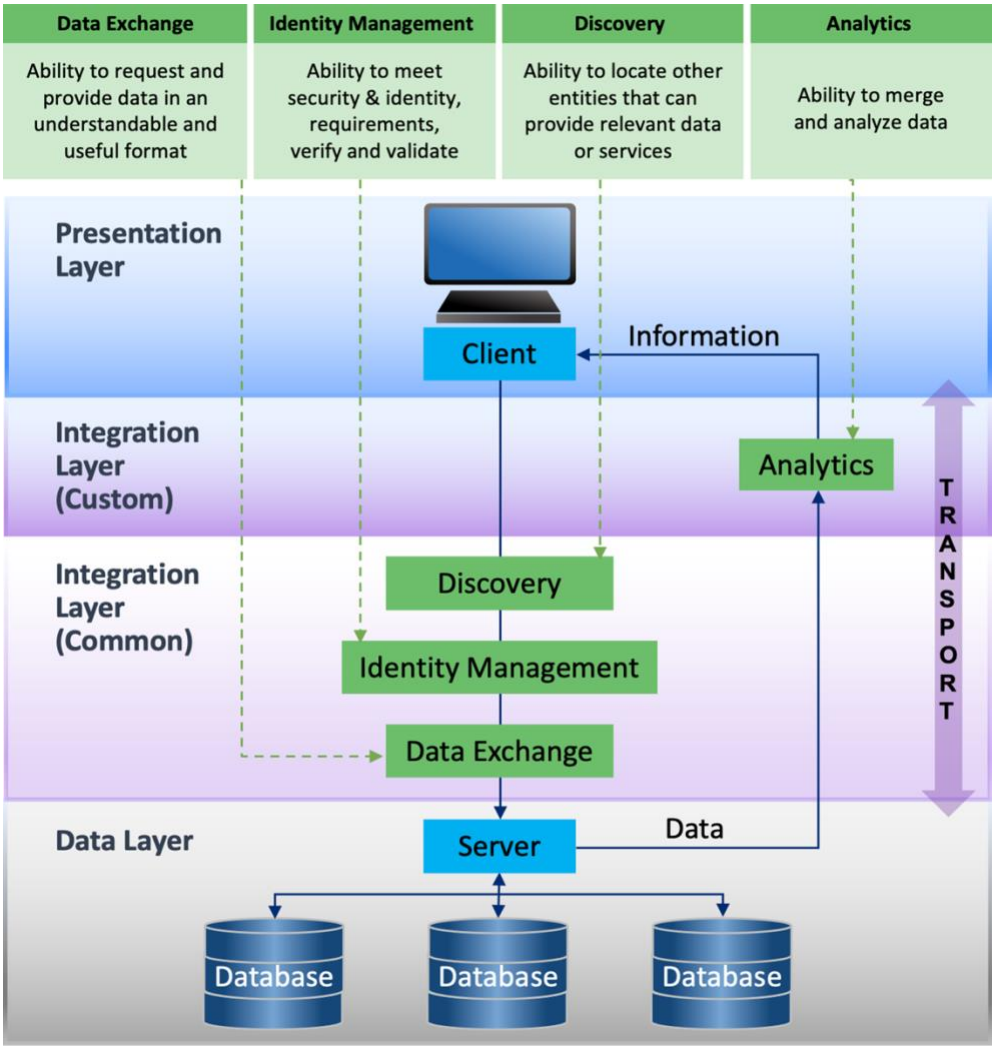


Figure ES-3: Expanded Conceptual Data-Information Model

As described in the National Public Safety Telecommunications Council (NPSTC) June 2019 *"Public Safety Internet of Things (IoT) Use Case Report and Attributes,"* we are in the midst of a rapidly growing technology environment in which Internet-connected devices are capable of reporting environmental data, biometrics, tactical data, location, and a wealth of other information. These devices will be carrying data over new transport paths (such as the National Public Safety Broadband Network [NPSBN]) and will be received by a number of Emergency Communications Centers (ECCs) such as: Public Safety Answering Points (PSAPs), Traffic Operation Centers (TOCs) found in Transportation Agencies, Emergency Operation Centers (EOCs) in Emergency Management Agencies, Operation Control Centers (OCCs) in Transit Agencies, Real Time Crime Centers (RTCCs) in Law Enforcement agencies, and even Fusion Centers. Each of these entities, while serving a different

purpose, has a similar challenge in bringing together data from disparate sources in order to gain visibility into their operational environment and develop improved insights from the collective view. The various sources of data, from agency legacy systems or new IoT devices, makes for a very complex public safety communications ecosystem. The Information Sharing Framework seeks to provide guidance on how to analyze that system and assemble the necessary components for improved interoperability.

It is important to note that the ISF is *not* meant to replace other relevant interoperability guidance such as the National Emergency Communications Plan (NECP), the NG911 Roadmap, the National Interoperability Field Operations Guide, and the SAFECOM Interoperability Continuum, but rather it is meant to leverage and help ensure ongoing efforts support other key federal initiatives and partnerships. This document provides the groundwork for an approach that begins with a self-assessment to determine a public safety agency's readiness level to receive, integrate, and implement these advance capabilities as well as consider the agency's mission, resources, policies, and governance. It also includes basic requirements and capabilities to help support an approach that includes implementation guidance, use cases, recommendations to help influence standards, opportunities for public safety to test operational concepts, and applications to achieve an interoperable public safety ecosystem. As communication systems evolve over time, it is anticipated that this document will require adaptions and updates that align with and support public safety needs.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

In support of efforts to develop a framework for information sharing to support public safety telecommunications, SAFECOM and the National Council of Statewide Interoperability Coordinators (NCSWIC) in partnership with the Cybersecurity and Infrastructure Security Agency (CISA) have established the Information Sharing Framework Task Force (ISFTF) comprised of a number of information technology (IT) and public safety communications subject matter experts from agencies across the country. CISA is engaging with the ISFTF to develop an Information Sharing Framework (ISF) to ensure the effectiveness of new products and technologies as agencies transition to mobile and fully interconnected environments.

In 2018, CISA developed an architectural framework to support information sharing within the public safety community under the guidance of the ISFTF. Phase 1 of this effort was completed during the fall of 2018 with the delivery of a report describing the nature of the interoperability problem and identifying a high-level concept for visualizing the emerging public safety architecture. Phase 2 to develop more detailed guidance on a systems/enterprise approach began in May 2019. To date, a draft Concept of Operations document based upon public safety use-cases developed by the National Public Safety Telecommunications Council (NPSTC) has been delivered and distributed to participants in the ISFTF. The goal of Phase 2 is to transition the Phase 1 framework into a more comprehensive and usable multi-dimensional process that can be readily applied by any public safety agency in the United States.

The ISFTF objectives are to advance information sharing and interoperability for public safety agencies through:

- Developing an **information sharing framework** that expands beyond single organization focus
- Ensuring ongoing **engagement with peers** for feedback, best practices, and lessons learned
- Identifying **desired information flows** between networks, applications, services, and devices
- Providing insight and information to **help evolve technical and operational standards**
- Developing **recommendations and a roadmap** to help close **interoperability gaps**
- Identifying **best practices** for cyber security and interoperability in Internet Protocol (IP) environments based on standards and/or other solutions leveraging new big data players
- Integrating **lessons learned** from existing pilots and exploring new **pilot opportunities**
- **Socializing the ISF** with private sector partners for adoption and implementation

The ISFTF objectives ultimately support interoperability as well as the integration of new technologies and services into existing public safety communications ecosystems. These ecosystems (Figure 1-1 and Figure 1-2 below), which include the functions of public safety personnel, are dynamic multi-directional information exchange environments in both urban and rural settings and are becoming increasingly complex such that a single public safety agency cannot achieve communications interoperability and continuity alone. In addition, the demands for real time situational awareness surrounding an emergency event requires multi-jurisdictional and multi-agency information sharing. As a result, achieving effective interoperable communications now requires partnerships, such as the ISFTF, to ultimately help public safety achieve interoperable, integrated, secure, and timely situational awareness.

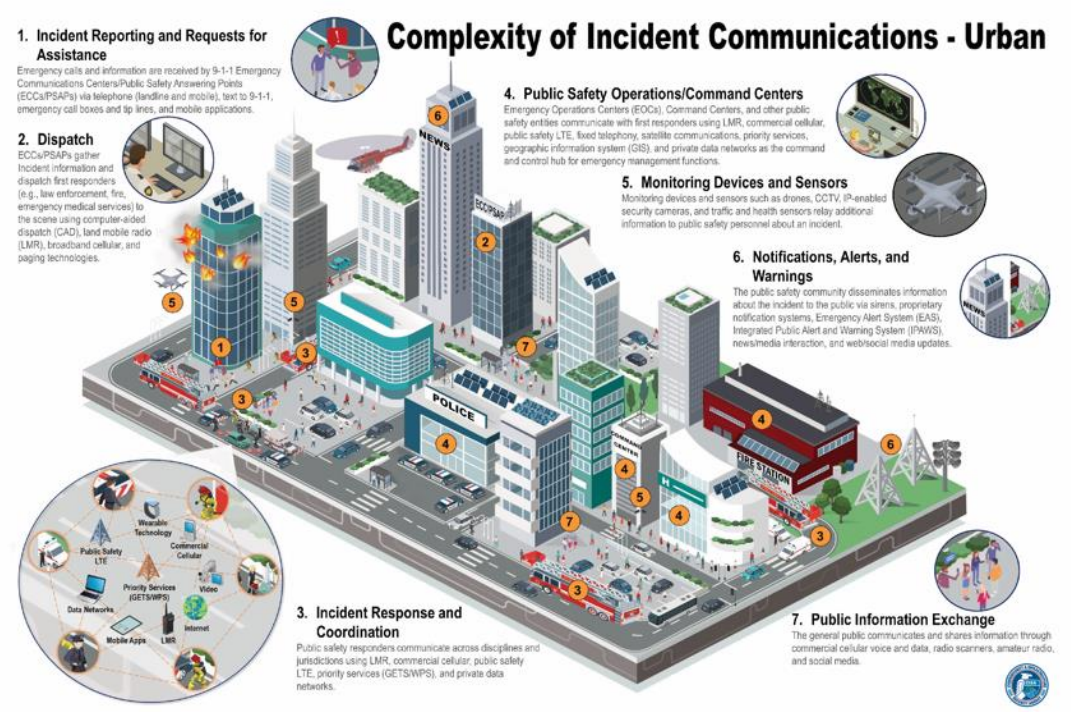


Figure 1-1: Complexity of an Emergency Communications Ecosystem in an Urban Environment

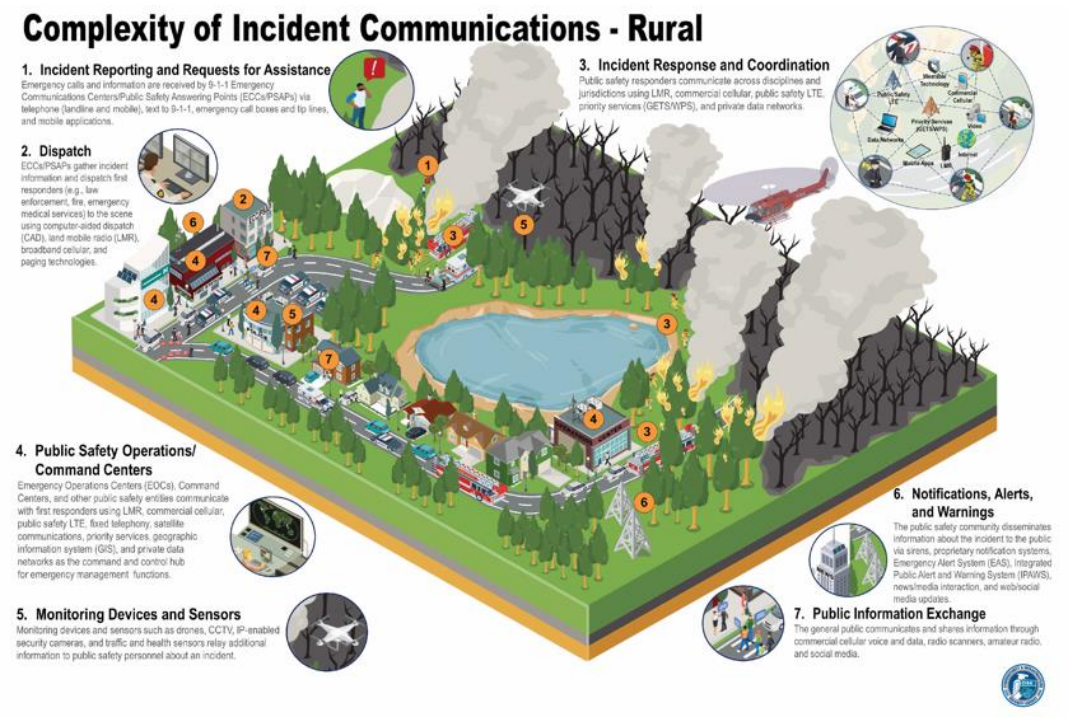


Figure 1-2: Complexity of an Emergency Communications Ecosystem in a Rural Environment

CISA has worked to ensure that the public safety community's firsthand knowledge of challenges, needs, and best practices are reflected in the National Emergency Communications Plan (NECP). The NECP is the Nation's strategic plan to strengthen and enhance emergency communications capabilities. In developing the NECP, CISA conducted the SAFECOM Nationwide Survey in 2018 in which thousands of public safety agencies and

organizations participated. Additionally, CISA used an extensive stakeholder engagement process to identify challenges and propose initial solutions to help improve emergency communications.

The NECP establishes a shared vision for emergency communications and is aimed at assisting public safety personnel who plan, coordinate, invest in, and use operable and interoperable communications for response and recovery operations. This includes traditional emergency responder disciplines and other partners from the community that share information during incidents and planned events. Figure 1-3 summarizes the NECP goals, of which the ISF will directly support Objectives 5.1, 5.2, & 5.3.

Figure 1-3: Summary of NECP Goals

2 DOCUMENT ORGANIZATION

This document proposes a high-level ISF that should be useful to both public safety practitioners and information technologists charged with making public safety data and communications systems more interoperable. During emergencies, sharing data within and across agencies (fire, police, EMS, transportation, utilities, etc.) and jurisdictions (e.g., federal, state, local, tribal, territorial, and municipal) is essential to successfully responding to and recovering from the emergency.

This document is intended to be a reference source principally for Statewide Interoperability Coordinators (SWICs) and other state and local level public safety communications personnel who work with land mobile radio, cellular broadband, 911, and state public alerts, warnings, and notifications systems, and any personnel directly involved in acquisition, management, and oversight of public safety data and communication systems. It may also prove useful to federal government personnel in similar roles as it addresses the issues associated with sharing data within and across public safety agencies.

Given the scope of this effort and for clarity's sake, the document was structured in such a way as to present the information sharing framework concept in the body while providing the details and specifics of certain aspects of interoperability in the appendices. In general, public safety leaders and practitioners will benefit from content located in the body of the document while more technically oriented personnel (e.g., information technology practitioners and technology developers) may benefit more from the appendices.

The overarching goal is to provide a framework and vernacular that both practitioners and technologists can jointly relate to and use to support collaboration in developing requirements and architectures for more interoperable public safety systems. While public safety personnel generally understand the importance and need for increased interoperability, there is limited specific guidance on how to collaboratively assess and develop such systems, and much of the current guidance does not address all system components (i.e., credentialing, cybersecurity, transport, standards, etc.). The ISF proposes a systemic approach to facilitate understanding of how the specific elements support the larger system. The ISF is not intended to replace or compete with existing guidance, but rather compliment those efforts and broaden the understanding of how to design and implement more interoperable systems.

This document is composed of the following sections: [*Note: use "CTRL + click" on the bold title of a section or Appendix to navigate to that area of the document*]

- **Section 1 - Introduction** provides the role and objectives of the Information Sharing Framework Task Force (ISFTF).
- **Section 2 - Document Organization** provides a description of each section of this document, and where appropriate the intended audience for that section.
- **Section 3 - Background** provides an overview of the phased approach to the project and an overview of baseline work accomplished in Phase 1.
- **Section 4 - Information Sharing Framework** provides a high-level overview of the approach for developing and implementing an information sharing framework.
- **Section 5 - Summary** provides a high-level summary of the information found within the body of this document.
- **Appendix A - Baseline Technological Assessment** presents the results of a baseline technological assessment of emerging technologies and best practices. It includes discussion of several aspects of the technology-related components and their implications with respect to interoperability. It is a relatively technical appendix ***intended for readers who are interested in a deeper understanding of the technological aspects relevant to achieving interoperability***.

- **Appendix B - Use Cases** presents information on a sampling of representative use cases in public safety adapted from the 2019 NPSTC Public Safety Internet of Things (IoT) Use Case Report and Assessment Attributes. It illustrates how a use case can be disassembled into a sequence of actions from which system requirements can then be derived to help develop baseline functional and technical requirements. These requirements can then be used to perform a readiness level assessment, to evaluate framework solutions/options, and to support iterative testing and evaluation. This appendix is ***intended for both operational and technical public safety personnel***.

- **Appendix C - Policy Considerations** provides a discussion regarding the policy considerations that should be considered in the implementation of the ISF. This appendix is ***intended for all public safety personnel with decision making roles and responsibilities.***

- **Appendix D - Functional and Physical Architecture Approach Overview** provides a more technical understanding of the interoperability needs of the end-user and the technology community. This appendix is ***intended for use by the public safety IT community.***

- **Appendix E - ISF Implementation Cycle** provides examples, questions, tools, and resources that can act as guides for how to successfully complete each of the six (6) steps of the ISF Implementation Cycle. This appendix is ***intended for use by public safety personnel who have responsibilities for implementing interoperability programs (e.g., acquisition, training, CONOPS development, etc.).***

- **Appendix F - Acronym Lists** provides a list of acronyms and definitions used in this document as well as a list of common emergency communications acronyms.

3 BACKGROUND

The ISF project is being implemented using a systems engineering phased approach which allows for an iterative development process driven by the ISFTF and other subject matter experts. The ISF project integrates ongoing ISFTF feedback, employs use cases to update and track requirements, and identifies opportunities to validate efforts with operations personnel in the mission-based environments. Figure 3-1 below provides a notional timeline for project implementation.

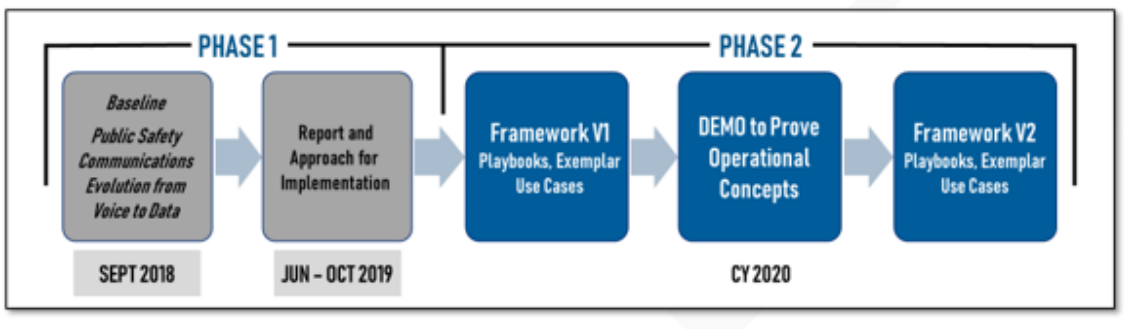


Figure 3-1: Notional Timeline for Project Implementation

3.1 PHASE 1

Efforts during Phase 1 initially focused on developing baseline documents summarizing the outcomes of a study performed for CISA in 2018. These documents provide a characterization of the capabilities and limitations of the existing public safety communications architectures. The report from this effort identified on-going initiatives (such as the National Public Safety Broadband Network (NPSBN) and Next Generation 911 (NG911)) and emerging technologies (including fifth generation technology standard (5G) and artificial intelligence), as well as the critical gaps and challenges that must be considered for interoperability. It also introduced the underpinning components of *people, processes, and technologies* that must be considered for any successful interoperability effort.

Another foundational concept introduced was the logical, 3-layered model for the emerging information sharing ecosystem. This construct showed how disparate *data* systems' output is transported via networks to an *integration layer* where the data is processed, aggregated, manipulated, and analyzed as appropriate. The integration layer transforms the data into more readily consumable information, which can then be transported and distributed to the *presentation layer* for public safety end users' improved situational awareness and decision making. (Figure 3-2). The key to this transformation is developing and utilizing an integration layer that performs the necessary functions to adjudicate and mediate between existing legacy agency data systems and end users' applications in the presentation layer while also providing the necessary cyber security functions to ensure the safety and security of shared information.

This concept is a pragmatic approach to the data interoperability challenge in that it recognizes and accommodates the fact that legacy data layer systems were typically not designed to share information outside that system or agency. Expecting those systems to be revamped for improved interoperability and data sharing is not realistic nor scalable. Similarly, the presentation layer utilized by public safety is increasingly a wireless smart device consuming data via an application. Thus, the data layer and presentation layer systems have largely been defined by widespread adoption of the existing hardware/software solutions by both the public and the public safety communities. In order to provide data from legacy systems to the increasingly remote/mobile end users requires that an integration layer set of functions be provided to translate between the data and presentation layers. The integration layer also provides transport across different networks, such as fiber, LMR, and cellular services, in order to access this integration layer in various locations where the data is processed, aggregated, manipulated, and analyzed to eventually become actionable information for the end user in the presentation layer.

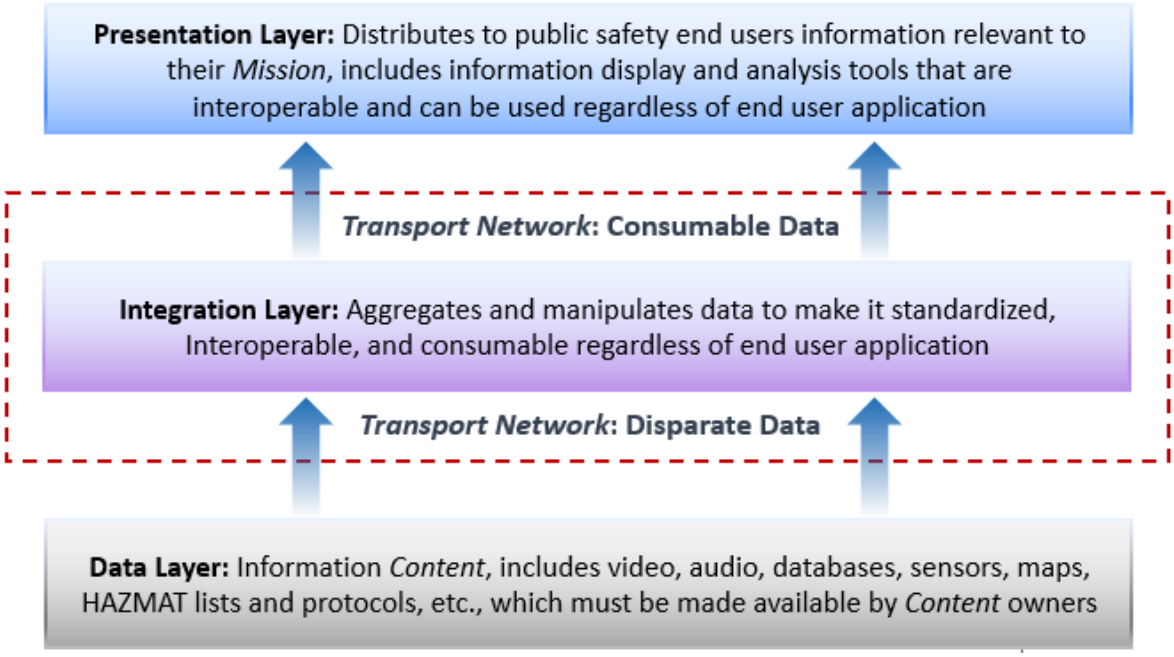


Figure 3-2: Conceptual Data-Information Model

The Phase 1 effort developed a knowledge product that identifies and delineates the following guiding principles with corresponding core needs for a public safety ecosystem (also summarized in Figure 3-3):

- *Interoperability*
  - Interoperability that includes all data types (*video, text-based, audio, and sensor*)
  - Interoperability between disciplines and jurisdictions, regardless of acquisition types
  - Interoperability with systems from other partnering agencies (e.g., private sector, volunteer organizations, etc.)
  - Interoperability between devices and applications
  - Supports an inclusive people, processes, and technology emergency communications ecosystem
- *Trust and Security*
  - Alignment with a standards-based Identity, Credential, and Access Management (ICAM) solution for multi-level, need-to-know credentialing that protects content, content ownership, and content management privileges
  - Implementation of the Risk Management Framework (RMF) to provide secure and resilient cyber security solutions that detect, respond, mitigate, and recover from existing and emerging cyber threats to existing and future interoperable emergency communications
  - Extended secure access across services and jurisdictions, to include third party data
  - Cyber security and credentialing measures to protect information from unauthorized access
  - Protection against emerging threats, including IoT and other endpoint devices-related attacks
- *Resiliency*

- Route diversity to ensure routing communications between two points over more than one physical path with no common points of failure
- Redundancy to ensure that additional or duplicate communications assets share the load or provide back-up to the primary asset
- Priority Services to enable continued communications access even in times of high use and congestion
- Protective/restorative measures to decrease the likelihood that a threat will affect the network, while restorative measures enable rapid restoration

- *Data Management*
  - As new technologies continue to emerge, there is a need for advanced data management systems with analytical and automation capabilities to ensure the right information is received at the right location at the right time.
  - Discovery of and access to such a large amount of information will pose significant challenges to avoid overwhelming end users with information beyond what is needed for decision-making requirements.

Interoperability	Trust & Security	Resiliency	Data Management
▪ Across jurisdiction and between agencies ▪ Across networks, especially LTE and LMR ▪ Between devices ▪ Improved access to third party data ▪ Between mission critical voice and data services ▪ Across applications	▪ Develop trusted components, engineer cyber resilience upfront ▪ Verify trust cross-jurisdictions and between agencies ▪ Protect data ownership and user integrity while enabling need-to-know based access ▪ Anticipate and thwart emerging threats, including IoT	▪ Priority services ▪ Ability to augment networks with ad hoc capability ▪ Redundant communications capability ▪ Scalability to respond to larger incidents ▪ Recovery capability	▪ Ability to consume large amounts of data ▪ Making data discoverable, accessible, and consumable ▪ Ability to assess utility and validity of data ▪ Ability to store data for forensic analysis

Figure 3-3: BASELINE Capabilities Identified by the ISFTF

These guiding principles should be the key considerations in any ISF architecture within a public safety organization and should also drive capabilities and requirements for any product or service acquired to support that architecture.

Consistent with the people/process/technology (enterprise) approach, the second component of Phase 1 began in June of 2019 and was based on the following three components:

- Employment of a *people-oriented approach* with the creation of the ISFTF of public safety experts who help to inform the effort
- A process or *functional-based approach* for deconstructing use cases into functional entities along with their required information needs and driving information sharing to help facilitate further input and requirements from the ISFTF and other stakeholders
- A *technology-based approach* to identify the emerging technologies, solutions and best practices that address identified gaps in information sharing today based on the above functional approach

This combination of enterprise-based approaches enables the identification of capabilities that align with mission needs and operational practices, allows for iterative, stakeholder-driven development of reference architectures and solutions, and identifies opportunities to exploit the full capabilities of emerging technology.

The final effort under Phase 1 included the adoption of the use cases[1] from the NPSTC (Figure 3-4). These eight use cases were selected as being adequately representative of the range of incident scale events that public safety routinely deals with (from local, to regional, to statewide or national scale event [see Figure 3-5]).

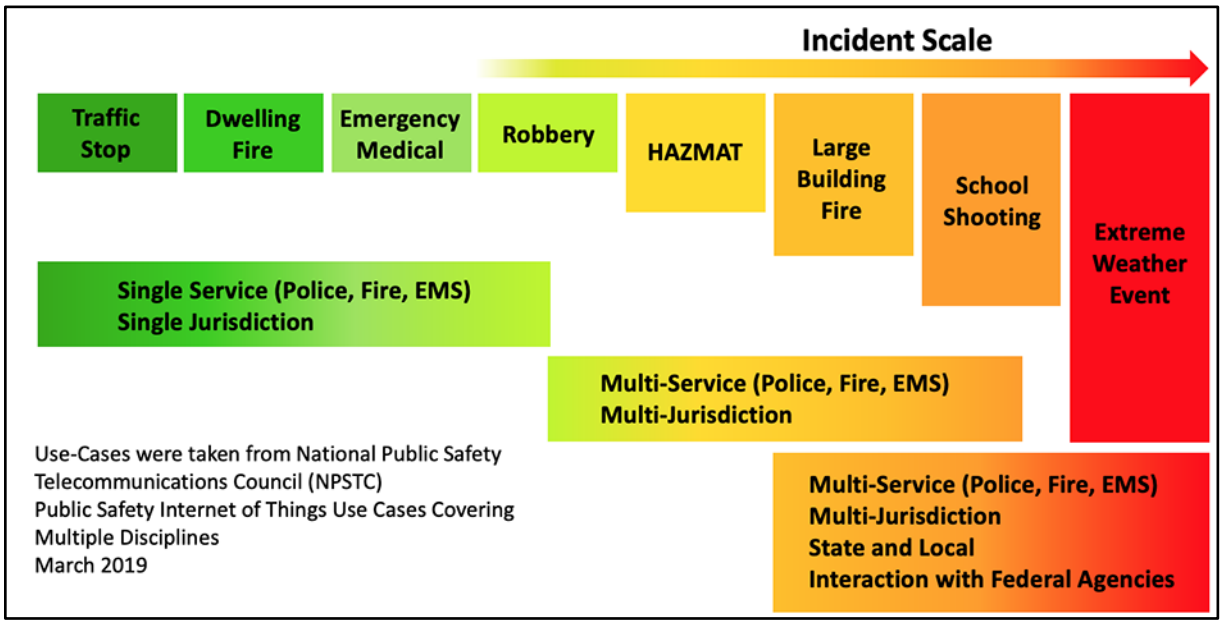


Figure 3-4: NPSTC Use Cases

[1] https://www.npstc.org/download.jsp?tableId=37&column=217&id=4195&file=NPSTC_PSIoT_Use_Cases_Report_190616.pdf

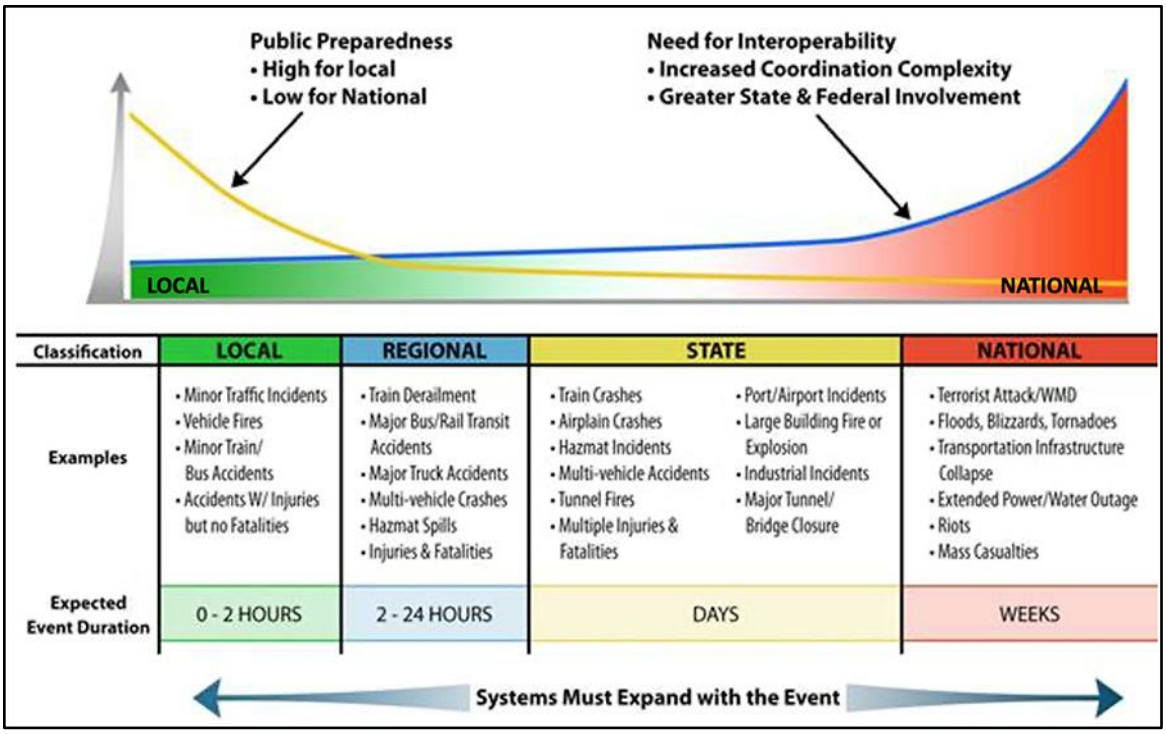


Figure 3-5: How Incident Scale Determines Public Safety Response

These use cases will also be used to help a) organize the discussion, b) ensure that a wide range of aspects of public safety response have been considered, and c) serve as a starting point to develop baseline functional and technical requirements. These requirements will then be used to help assess architectural alternatives and solutions as well as to support iterative testing and evaluation for both bench and field testing. These use cases are fundamental to developing the functional architectural view of the ISF, revealing the different types of entities involved in public safety events along with their unique sources and needs of information. This functional view will identify and codify the functional exchanges, which endure over time, to ensure the right types of information are provided to the right types of entities at the right time.

4 INFORMATION SHARING FRAMEWORK

4.1 DOCUMENT PURPOSE

This document provides a baseline for the development and execution of the ISF. The overarching goal of the ISF is to inform and guide the transition to a common information exchange approach that a public safety agency can adopt and use efficiently to make its ecosystem more interoperable. The ISF approach to addressing interoperability is based on a proven approach of defining interfaces and interoperability between enterprises. It includes several architectural views including:

- A *logical layered model* of data and information that can depict and demonstrate how disparate raw and processed data is managed and shared (3-layer model);
- A *functional information exchange model* that depicts the types of entities involved in public safety along with the functional exchanges that are required to happen among those entities in order for them to perform their mission(s) efficiently and effectively and that are enduring over time; and
- A *physical interface model* that incorporates the above two models and provides a more tangible description of how the public safety entities need to interface using multiple but related dimensions which include applications, information services, devices, networks, and facilities.

This document also includes basic operational requirements and capabilities developed using the NPSTC June 2019 *Public Safety Internet of Things (IoT) Use Case Report and Attributes* report. These requirements and capabilities, as they mature, will drive the functional architecture view that will in turn inform and guide recommendations in the physical view to help evolve standards and opportunities for public safety agencies to test operational concepts and applications to achieve an interoperable ecosystem.

As the ISF evolves, it will also include components that support and integrate with other key federal efforts and documents such as the NECP and the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) Next Generation First Responder (NGFR) Integration Handbook, which identifies standards, interfaces, and data flows that would allow public safety agencies to integrate hardware, software, and data from different technology solutions and build their own public safety system.

4.2 KEY TERMS

- **Data** – Raw, unprocessed, unorganized material (machine readable)
- **Information** – Data that is processed, organized, and presented to provide meaning (human understandable)
- **Enterprise Architecture** – A comprehensive conceptual model that maps functional capabilities to physical structures to support the flow of information across the enterprise to achieve its mission. This document focuses on the identification of critical information exchanges between entities within the public safety enterprise architecture.
- **Architectural Framework** – Architectural framework refers to a limited set of architecture views that include logical, functional, and physical views to inform and guide the development of common standards, capabilities, services, and governance required to achieve an emergency communications ecosystem. This document will begin to describe the functional and physical aspects of the framework.
- **Communications Infrastructure** – Communications infrastructure refers to actual physical communications systems (e.g., hardware, antennas, devices, software, etc.).
- **IoT** – Network of physical objects or things such as sensors, electronics, software, electronics, and the network connectivity that enables these things to collect and exchange data. IoT connectivity promises significant benefits for public safety, including:
    - Improved Situational Awareness
    - Enhanced Common Operating Picture

- Improved Responder Health and Safety
- Efficiency and Cost-Saving Benefits
- Improved Access to Potentially Lifesaving Information

4.3 ISF SCALE

It is important to understand that for public safety, near real time situational awareness is essential. Additionally, situational awareness does not generally come solely from the information that can be provided by one system. In order to have a comprehensive understanding of the current situation, information must be shared between systems and agencies. The scale of an incident can span from a local single incident to a larger more complex national event; therefore, the requirements of an interoperable system will also have to reflect these different scenarios. The Incident Scale schema in Figure 3-5 characterizes the scope of the response to an incident as Local, Regional, State, or National. This characterization will have a bearing on the number and type of agencies responding.

Incident scale is directly associated with the level of public preparedness for a given type of incident as well as the complexity of the response coordination. Thus, incident scale determines the complexity of the response and the need for interoperable communications with the goal of near real time situational awareness.

4.4 ISF AND THE SAFECOM INTEROPERABILITY CONTINUUM

Developed with practitioner input from CISA's SAFECOM program, the Interoperability Continuum is designed to assist emergency response agencies and policy makers to plan and implement interoperability solutions for data and voice communications. This tool identifies the five critical success elements that must be addressed to achieve a sophisticated interoperability solution: governance, standard operating procedures, technology, training and exercises, and usage of interoperable communications (Figure 4-1). The critical success elements introduced by the continuum are entirely consistent with the people/process/technology rubric introduced earlier and provide measures that an agency can use to assess their interoperability maturity. Therefore, it is important that the ISF incorporate the people/process/technology rubric as an underpinning component to leverage the SAFECOM model's five sub-areas. This will help ensure a balanced and measured approach as the framework progresses though its lifecycle, informing and guiding the implementation of methods of interoperability.

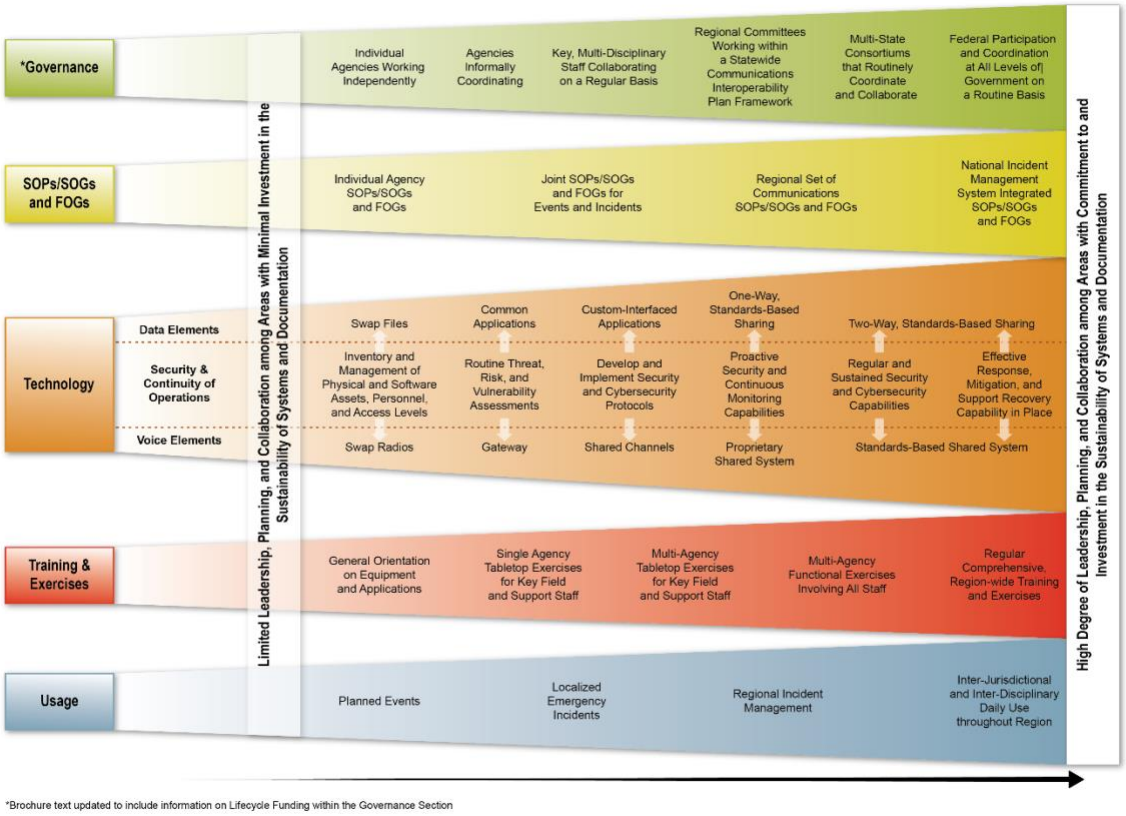


Figure 4-1: SAFECOM Interoperability Continuum

Interoperability is a multi-dimensional challenge. To gain a realistic picture of a community's interoperability, progress in each of the five interdependent elements must be measured. For example, when a region procures new equipment, that region should plan and conduct training and exercises to maximize the use of that equipment. Optimal-level interoperability is contingent upon individual agency and jurisdictional needs. The Continuum is designed as a guide for jurisdictions that are pursuing a new interoperability solution based on changing needs or additional resources; it is an evolving tool that supports national preparedness doctrine including, but not limited to, the National Incident Management System, the National Response Framework, and the NECP. To maximize the Interoperability Continuum's value to the emergency response community, SAFECOM will regularly update the tool through a consensus process involving practitioners, technical experts, and representatives from federal, state, tribal, territorial, regional, and local agencies. As updates to the SAFECOM Interoperability Continuum occur, the ISF will continue to align with these updates. The SAFECOM Interoperability Continuum will continue to be leveraged to help explain the ISF in a way that is familiar to non-technical public safety personnel or executives. The ISF follows many of the same concepts in the SAFECOM Interoperability Continuum, such as governance, standard operating procedures (SOPs), technology, training & exercises, and usage. Alignment between the SAFECOM Interoperability Continuum and the ISF will be required to ensure a common framework for Statewide Communication Interoperability Plans (SCIPs) and as a reference for future grant applications.

4.5 ISF Additional Considerations

Additional considerations during the development of the ISF include how the ISF transport function will support higher speeds for video streaming and near real time situational awareness applications, and how cellular technologies such as long term evolution (LTE), 5G, and beyond will impact the first responder and public safety community. Without greater bandwidth transport, advanced information processing, and enhanced analytic

capabilities, more information can become meaningless and actually cause more harm than good during a critical event.

It was also noted earlier how incident scale drives the need for improved interoperability due to the number of agencies and jurisdictions involved in larger scale events. A related factor involves whether an emergency incident is planned or unplanned. Planned events, depending upon the amount of advance notice, may provide the time needed to consider the data that is important to that event and put in place the necessary integration layer functions in order to share that data. With enough advance notice, preparing for a planned event may also allow for the study of the transport paths and additional deployable assets in order to balance the projected load by using historical data, pre-configuration of network policy/quality of service (QoS), priority, and preemption and address any spectrum conflicts/interference if that data exists and is available. The ISF provides guidance on how to approach those component needs and facilitate more specificity in the people, processes, and technology for planned events. Conversely, unplanned events provide a challenge in that there is a need for more ad hoc data sharing given the nature of those type events. However, the ISF still provides value for these type of incidents. If an agency is designing their data systems according to ISF principles (i.e., meeting the content owner responsibilities of making data discoverable and accessible, providing the ability to authenticate users, and the ability to publish their content in a consumable way), then even ad hoc sharing is possible with reasonable effort. Furthermore, unplanned events may provide challenges in particular for the transport function as the nature of the event may result in congested cellular infrastructure. However, this does not negate the ISF planning and design effort; rather it points out the need for an agency to preserve multiple transport options in order to remain resilient in the face of all type of incidents (those of various scale, planned or unplanned).

For the purposes of this document, the ISFTF catalogued data into the following: 1) Video, 2) Text-based, 3) Audio, and 4) Sensor. Each of these data types will have different standards that apply, different transport requirements, and depending on decision-making needs, this data may be treated very differently by end users. For example, text messaging is currently used for social interactions, but this capability could eventually be integrated into ECCs.

The communications operating environment must also be considered when implementing the three-layer interoperability approach. Achieving the benefits of full implementation may be relatively easy in an urban environment with robust transport capabilities (i.e., full internet, broadband, and fiber communications at the public safety community's disposal). However, a rural area with minimal pre-existing infrastructure or a communications compromised environment, which is common after natural disasters, may have more challenges in accessing and transporting relevant information to end users. The following describes three operational environments representative of a continuum from full access/capacity to limited access/capacity:

1. **Baseline Environment**: An environment in which access to the Internet or other communications infrastructure is readily available with little to no degradation and supports core information sharing
2. **IP Access Rich:** An environment that provides substantial Internet access that can still be stressed to support a wide range of interoperating systems
3. **Limited Access:** A critical environment where there is limited access due to a lack of infrastructure or damaged infrastructure. The most obvious example of an austere environment is following a natural disaster or other large-scale incident in which the communications or power infrastructure is damaged

Therefore, larger scale incidents, unplanned events, and limited access communications environments are additional considerations that will affect the ISF planning and design efforts.

4.6 ISF DEVELOPMENT

Figure 4-2 below provides a more detailed view of the logical (or layered) model as the underpinning for ISF. The challenge is to move data from the legacy systems in the data layer to the end user in the presentation layer. This is accomplished by developing the integration layer to perform a number of important functions such as: 1) Data Exchange, 2) Identity Management, 3) Discovery, 4) Transport, and 5) Analytics. The Common sub-

section in the Integration layer below suggests that certain functions should be widely applicable across datasets and systems. These functions encompass Data Exchange, Identity Management, and Discovery and allow for full interoperability regardless of the vendor chosen for the product or service being acquired. The Custom sub-section is where the Analytics function resides and still allows for some vendor differentiation while not violating the key outcomes of interoperability, security, resiliency, and data management.

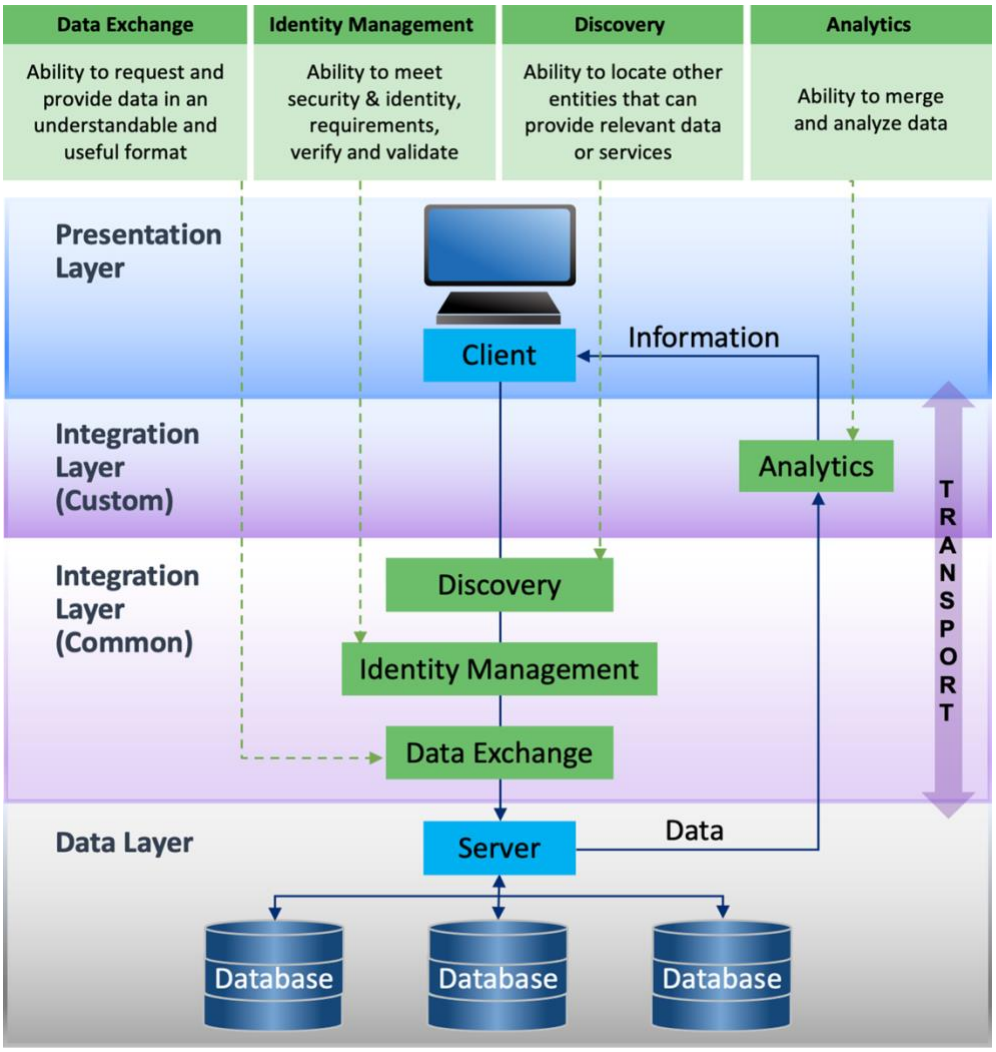


Figure 4-2: Functional Components of an Information Sharing Framework

In order to begin leveraging the functional components of the integration layer of the ISF, the public safety mission owner and content owner should be asking themselves high-level operational questions. Figure 4-3 through Figure 4-7 below takes these high-level operational questions, expands them, and aligns them to the various functional components of discovery, identity management, data exchange, analytics, and transport. These are the types of operational questions which must be answered to enable a public safety organization to share information with other organizations during a multi-agency, multi-jurisdiction event. The questions on the left side of Figure 4-3 through Figure 4-7 are questions to address with mission owners (public safety personnel executing the mission), while the questions on the right are questions content owners (the system owner whose information is needed for the mission) should ask themselves. Mission owners are end users consuming the information in the presentation layer, whereas content owner are the keepers of the data and provide access to the data layer where it resides.

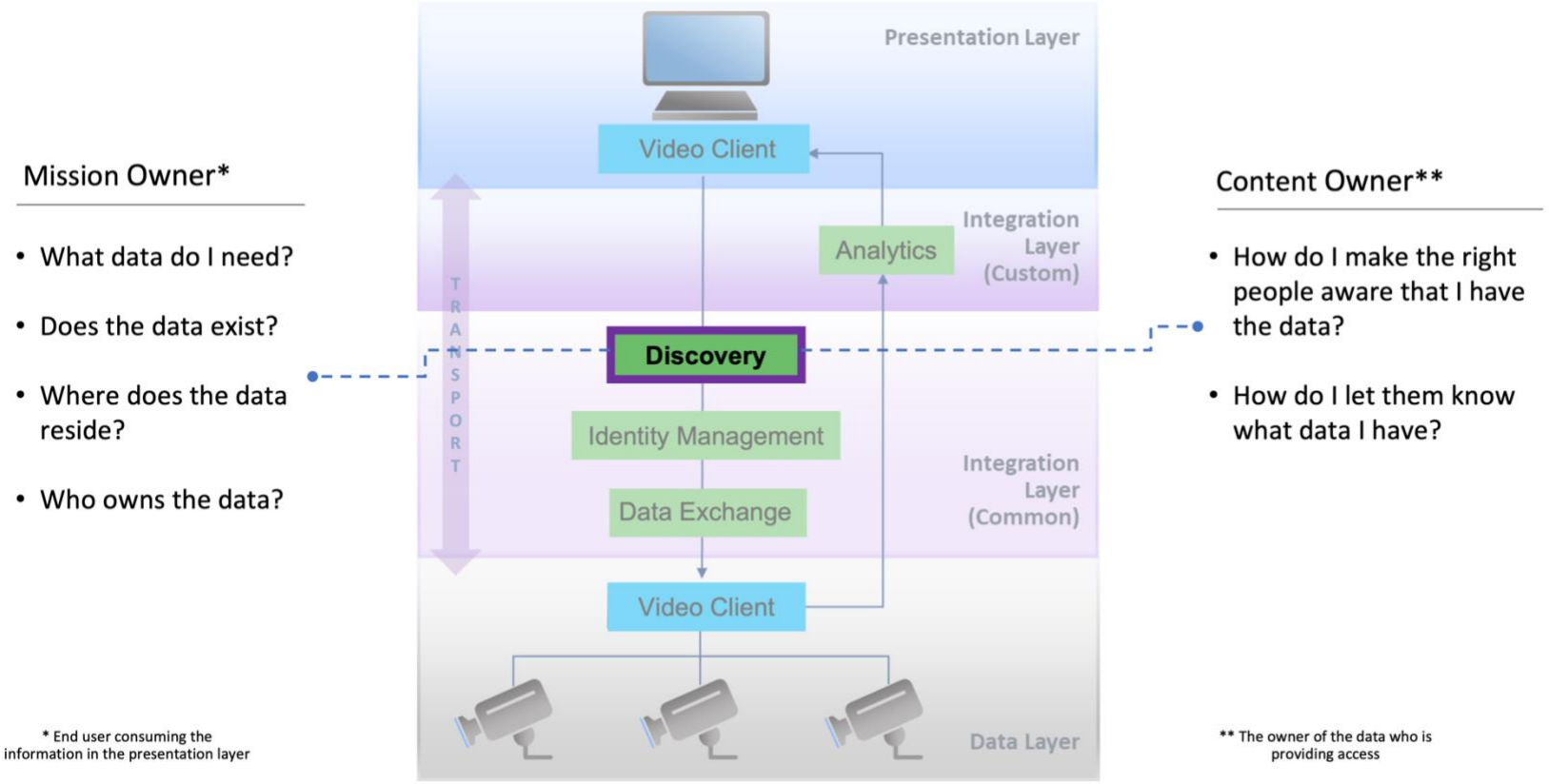


Figure 4-3: Discovery Operational Questions

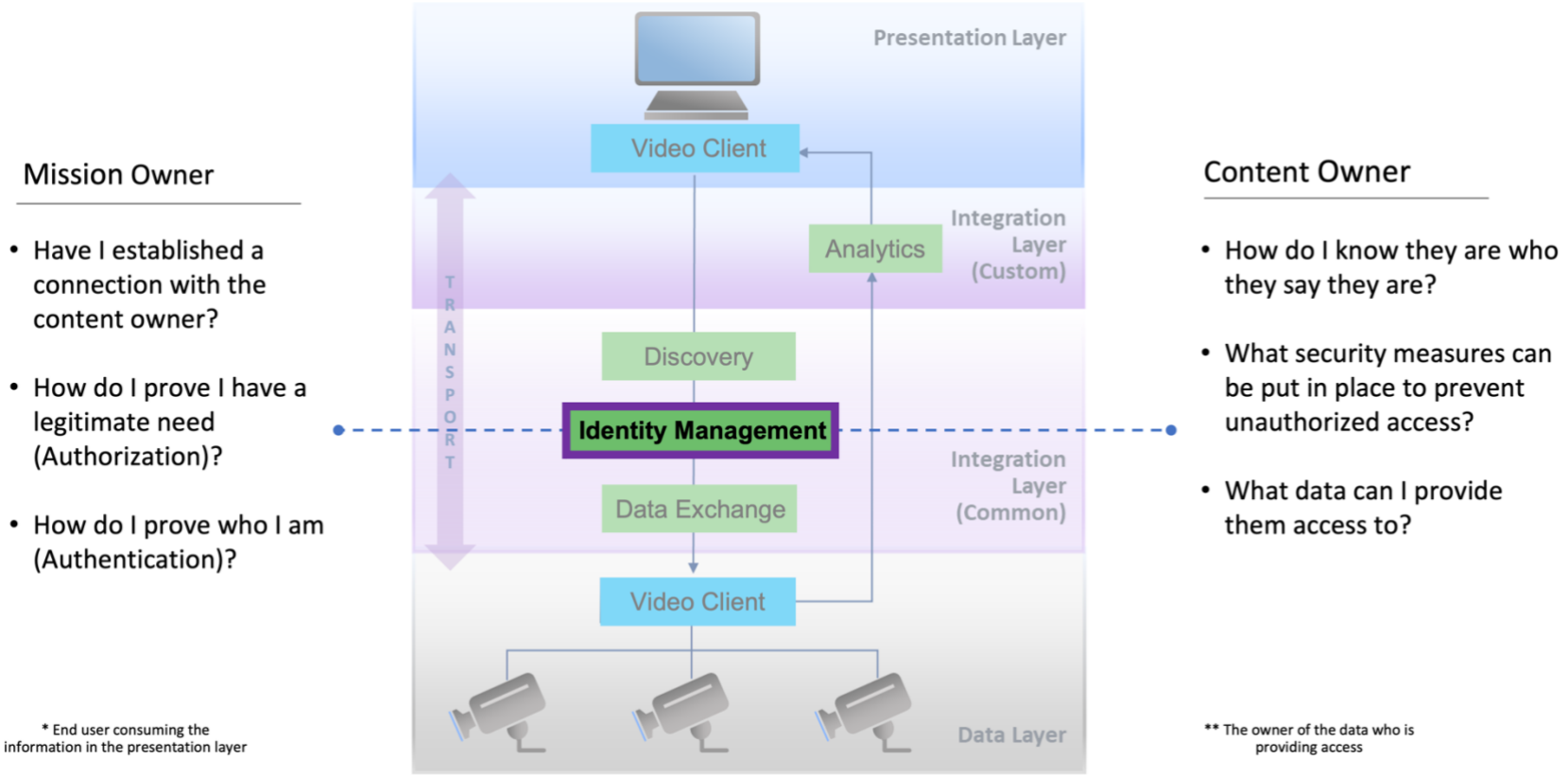


Figure 4-4: Identity Management Operational Questions

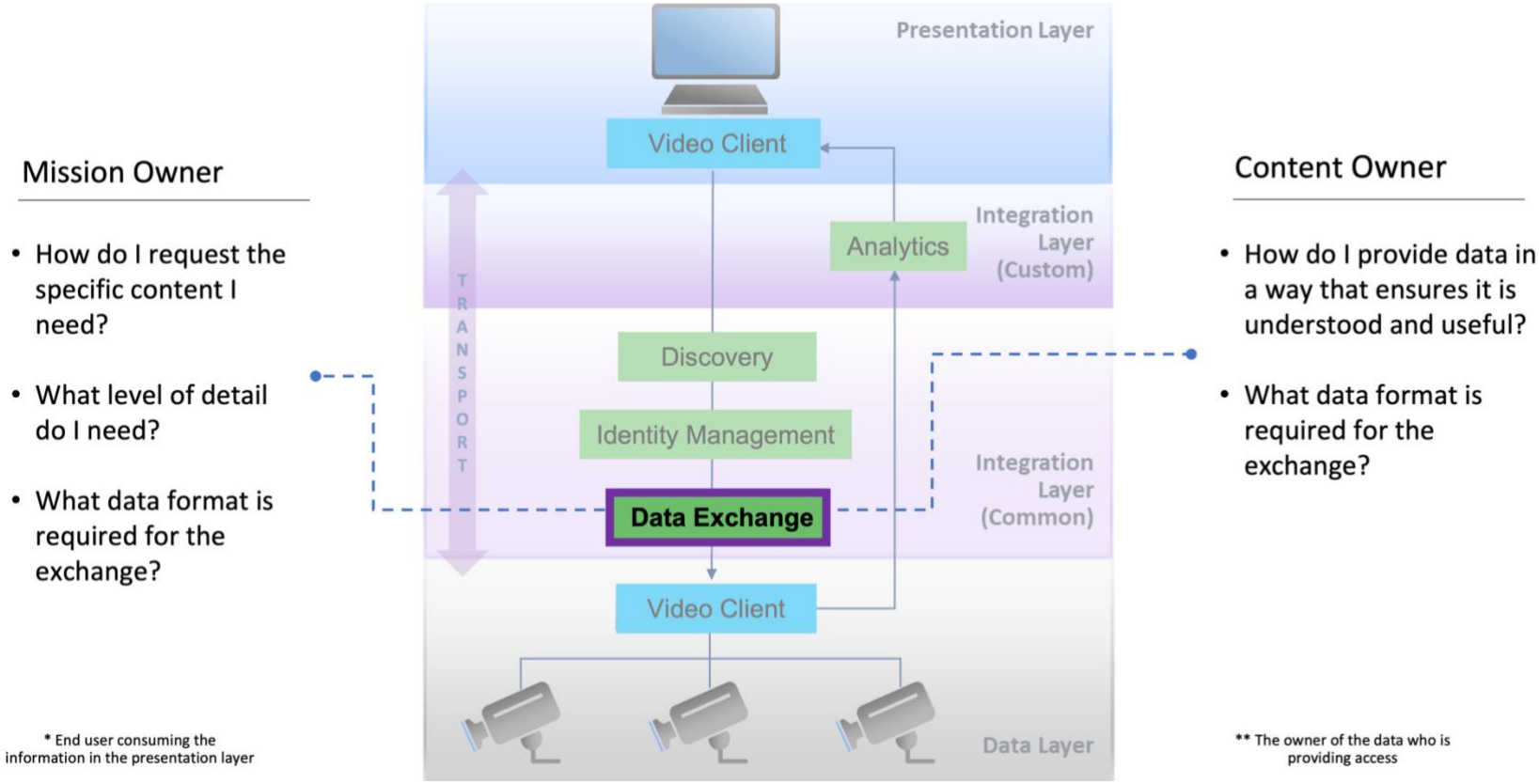


Figure 4-5: Data Exchange Operational Questions

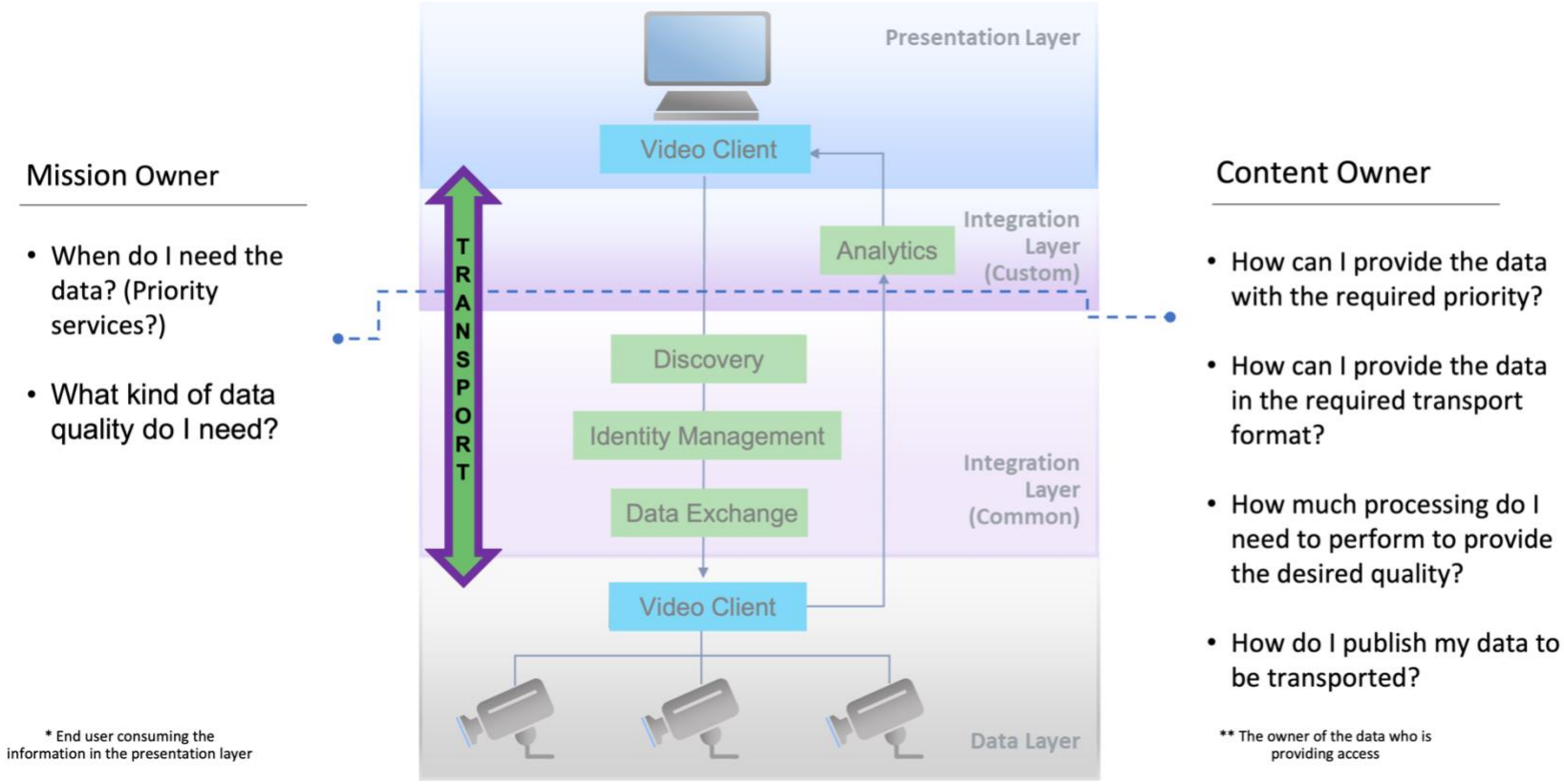


Figure 4-6: Transport Operational Questions

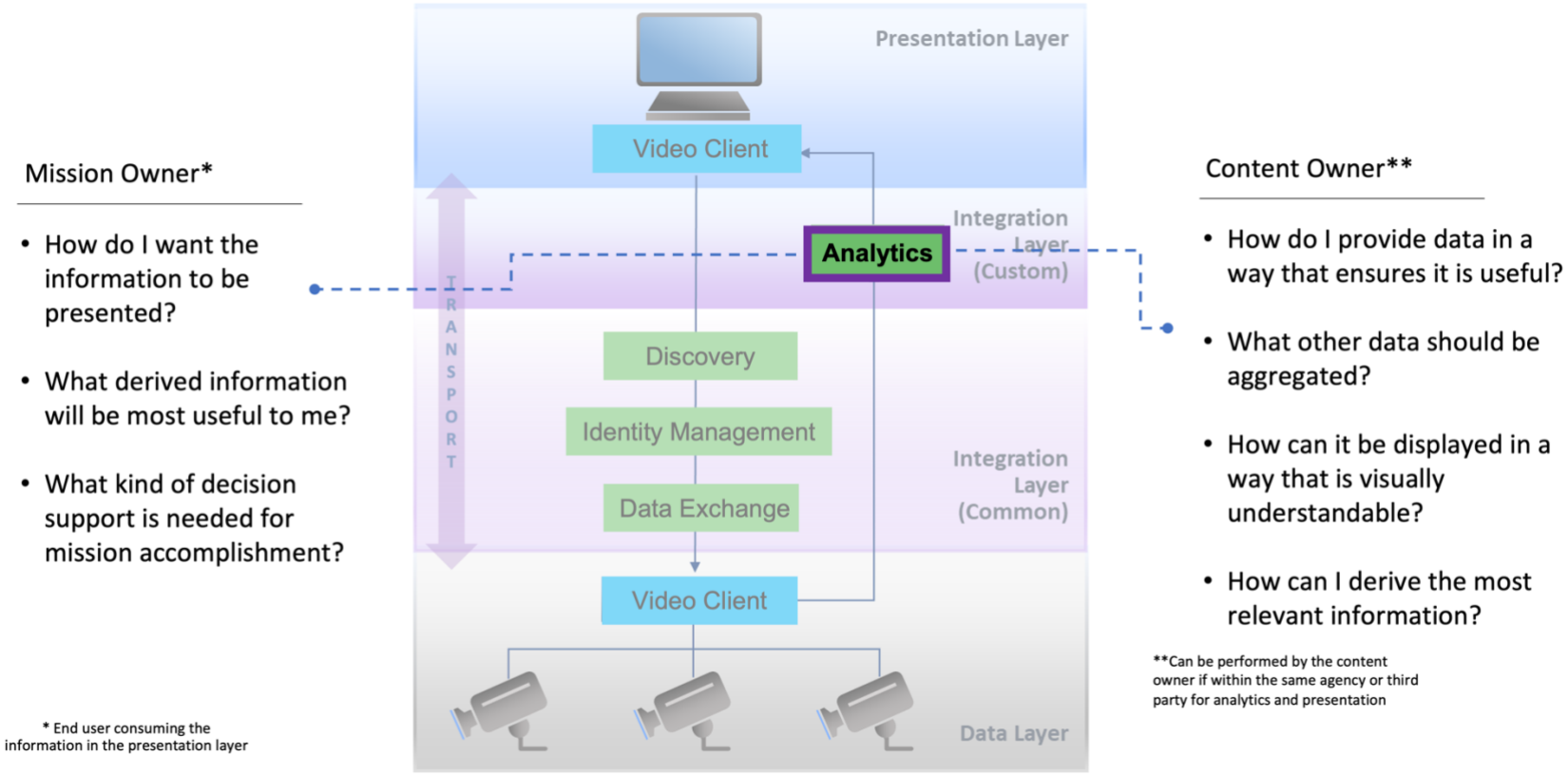


Figure 4-7: Analytics Operational Questions

As most public safety organizations will not be able to customize the ISF in isolation, certain existing external factors will influence the ISF development, such as implementation of a cyber-security RMF and ICAM, integration of LTE and LMR networks, existing network topologies of center to center connections (or lack of) to ECCs, NG911 architectures, and 5G and IoT products and services. In short, ***the ISF ecosystem, as applied to a particular agency or jurisdiction, requires determining the relevant data sets, where they reside, and how they can be accessed, aggregated, and securely transported to the right end user in a timely fashion so as to provide near real time situational awareness***. This requires an understanding and employing of a variety of tools and transport protocols in the integration layer to accomplish the desired level of interoperability.

Appendix A provides more technical detail into each of these transport networks, existing standards, and information sharing approaches in order to further development and customize the ISF as illustrated in Figure 4-8 below.

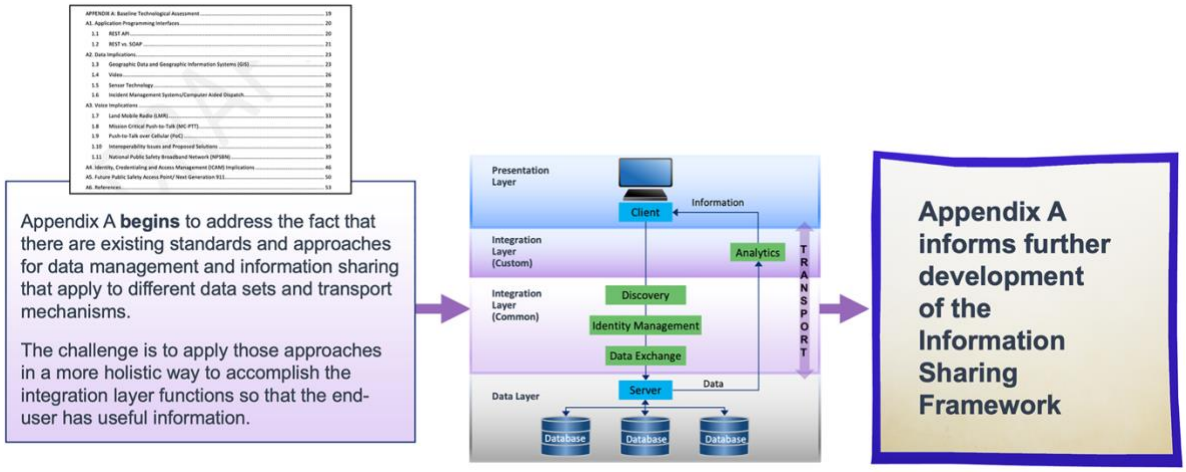


Figure 4-8: Technical Considerations for Data Integration

4.7 EXAMPLE CUSTOMIZATION OF ISF

As described in the previous section, there are many considerations that drive the implementation of the ISF. *Mission* is one of the most impactful drivers because it determines what data is required to help meet the mission and what entities need to work together to make it possible. Additionally, data *content* identifies what data is needed to accomplish the mission and therefore determines what technology enablers should be employed. And finally, the operational environment [baseline, IP rich or Limited] will determine what *transport* mechanisms need to be utilized. For example, sharing real time video data requires a high speed, high bandwidth transport mechanism that can only be achieved by particular technologies. Figure 4-9 describes how Mission, Content, and Transport influence one another and impact how the ISF will need to be designed and implemented for a particular public safety agency.

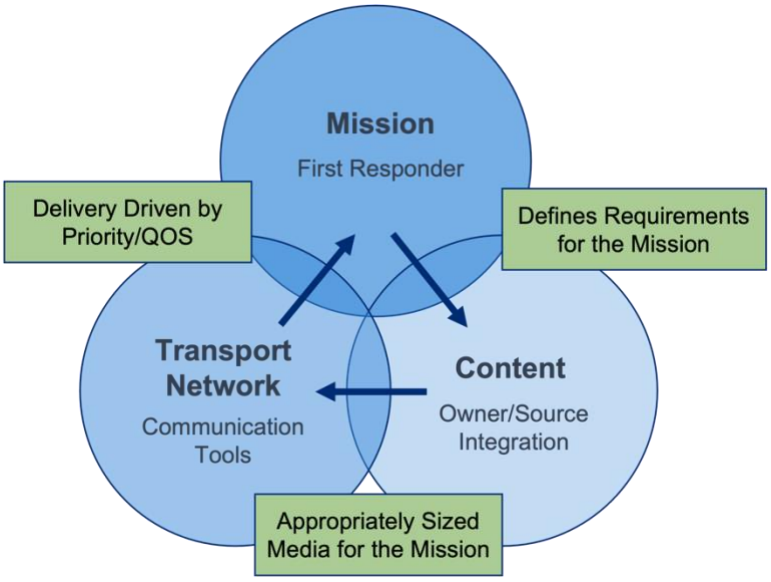


Figure 4-9: Mission Relevant Content

To further demonstrate how complex missions can affect content and transport requirements, the seventh use case (Active Shooter) (see Appendix B Section B.5.7) of the eight NPSTC use cases has been selected to illustrate how, as the use case progresses, mission needs change, stakeholder involvement evolves, and the data content and transport means become more complex (see Table 4-1).

A public safety entity should walk through their scenario as illustrated below to identify the stakeholders involved (depending upon incident scale), the mission requirements (what is the goal?) in each phase of the scenario, what information content is needed to accomplish the mission, and what transport mechanisms are available to move the data. Identifying these component parts is essential to constructing the necessary IT architecture to meet the operational need.

Table 4-1: Exemplar - Use Case #7 Active Shooter Timeline versus Mission, Content, and Transport Needs

Step	Description	Stakeholders	Mission	Content	Transport
1	A shooter enters a public school through an unsecured delivery entrance. The School Resource Officer (SRO) is in the parking lot checking parking passes. As the shooter moves through the hallways, he encounters teachers and students and fires several rounds injuring multiple people. Several nearby teachers contact the office using the in-classroom telephone reporting they hear sound of gunshots. Teachers and students call 911. The shooter continues through the school.	• Witnesses (Teachers & students) • SRO • ECC • School Office • Suspect (Shooter)	Notify the SRO (nearest onsite help) and gather intel about the developing situation	• Audio • Video • Text-based • GPS	• School Intercom System • Cellular • LTE • Satellite Link (GPS)
2	The ECC communicates with the SRO via LMR, advising the SRO of the location of the shooter so he can enter the school from a safe location. ECC personnel continue to receive multiple calls and have initiated the active shooter response protocol, and notifications are sent to police, fire, and EMS.	• ECC • SRO • Police • Fire • EMS • Suspect • Law Enforcement Dispatch	Mitigate the threat and protect the community involved	• Audio • Video • Text-based • Alerts to Police, Fire, EMS • GPS	• LMR • LTE • Cellular • Satellite Link (GPS)
3	Live streaming video and text messages from citizens. Due to expected injuries seen on the videos, hospitals are alerted.	• Witnesses • Local Hospitals • Suspect	Analyze the severity of injuries and prepare hospitals	• Video • Text-based • Alerts to hospitals	• Cellular • LTE
4	Incident command contacts ECC and request most recent blueprints for the school.	• Incident Command • Dispatch • School Record Owners	Locate the suspect	• Cellular • Text-based	• Cellular • Wi-Fi (Transfer documents)

Step	Description	Stakeholders	Mission	Content	Transport
5	School's surveillance camera system was recently updated so real-time video is being received by the company managing the system. Video streams from school cameras are provided to incident command who uses this information to advise responding units of the shooter's location. One of the video feeds detects a suspicious device in cafeteria hallway. Photos and video are provided to the local bomb unit for situational awareness and risk assessment.	• Camera System Owners • Local Bomb Unit • Police • Suspect • Incident Command	Utilize onsite video to identify suspect, track movement, identify injuries, and disseminate information to responders	• Video • Alerts • GPS	• LTE • LMR • Mobile Data Terminals (MDTs) • Satellite Link (GPS)
6	Mutual aid from surrounding jurisdictions requested. Unified command established and real-time video displayed and tracking the shooter as he moves through the school. An electronic blue print of the school is also projected for the IC	• Allied (Law Enforcement Mutual Aid) agencies • Suspect • Unified Command	Develop overall situational awareness and provide updates to responders.	• Audio • Text-based • GPS	• LTE • Satellite Link (GPS)
7	Analytical mapping capabilities are used to compare the location of the shooter via real-time video feeds with the electronic blueprint so the location of the shooter is known, as well as the locations of the injured victims. Incident Command contacts the ECC and requests unmanned aircraft system (UAS) support for streaming live video to monitor school exits in the event the shooter flees the building. UAS video is displayed for the unified command personnel.	• Dispatch, • Unified Command • Suspect	Identify exact location of suspect and survey school perimeter	• Video • GPS	• Radio Frequency (RF) (for UAS) • Satellite Link (GPS)

Step	Description	Stakeholders	Mission	Content	Transport
8	State Emergency Operations Center (EOC) activated to monitor the situation and be ready to send additional resources. Task Force Responders (TFR) from a neighboring county are communicating with command staff and told which parking lot entrance to use as they enter the school property for safety purposes. The TFR lead is provided a tablet with video feeds showing the injured and locations in the school. The TFR lead executes an application that retrieves data from electronic blueprints to help determine the exact location of the victims and the shooter within the school. TRF team is wearing body worn cameras, physiological sensors, and geolocation devices and have safely entered the school and begin extracting injured victims.	• TFR • State EOC • Unified Command • Victims • Suspect	Enable responders to safely extract victims	• Sensor • Video	• Sensor transfer (vendor specific) • LTE
9	The local Bomb Squad team is en route and evaluating video feeds from the school to assess the suspicious book bag that was located in the hallway by ECC personnel. Ongoing video feeds continue to inform incident command to ensure the TRF team remains a safe distance from the shooter while he is being pursued by officers. Triage, Treatment, and Transport (T-3) has been established outside the school by emergency medical services personnel. EMS also apply physiological sensors to victims so their vital signs can be monitored. The shooter is located and restrained. The Bomb Squad has safely rendered the suspicious book bag. The scene is processed and eventually cleared. Speech recognition software is used to log and submit incident reports.	• Local Bomb Squad • TRF • EMS • Suspect • Unified Command	Investigate bomb threat and restrain shooter	• Video • Sensor	• Sensor transfer (vendor specific) • LTE

4.8 How to Build Your Integration Layer

As discussed earlier, the mission defines the requirements. It identifies who needs what information (i.e. Data or Content), by when, in what priority, and in what format. The use cases (found in Appendix A) further illustrate how a particular public safety mission can be broken down into segments to identify what content is needed by which stakeholders as the event unfolds. The mission is the source of the information needs in the ISF.

The purpose of Figure 4-10 is to illustrate a more structured approach to applying the information sharing framework (ISF) concept. The terms used in the figure have all been described in earlier sections of this report (see Sections 4.6 and 4.7). This graphic further examines the integration layer functions of Discovery, Identity Management, Data Exchange, Transport, and Analytics and how one applies these concepts in light of the Mission/Content/Transport construct.

The remainder of Figure 4-10 walks the user through the thought process on how to identify the key components of the ISF and how they could be configured in a more detailed architecture that would be needed to build out a particular solution in a specific public safety setting. Each of the functions to be performed in the integration layer are discussed below:

- **Discovery** – Once the information (i.e. content) for a particular mission (i.e. use case) has been identified, that information needs to be discovered. The method to discover that content may vary from using available web-based search engines to consulting a particular database of sources of information (such as Earth cam for video sources). Discovering content within an agency by an agency employee should be relatively straightforward. For example, an employee may have an application on their issued smartphone that will provide access to agency data and systems. However, there will be missions in which data that is not controlled by the agency is relevant to the mission. One such example may be to identify a private camera that may have observed a crime scene that is not owned or controlled by the public safety agency. Mechanisms to address this specific example vary, including developing registries of private sector cameras in which a business owner may enroll. Regardless, public safety entities need to consider the content they may need to routinely access and take steps to facilitate how their employees may discover and ultimately access that data. Regional organizations, joint task forces, and interagency working groups are good forums to raise this issue of data sharing and access.

- **Identity Management** – Once the needed content has been discovered, the end user would need to access that information. In order to do so, they must have rights in the system where that data resides. This often takes the form of an account with a username and password. It would be best that these systems extend public safety access prior to the immediate need of an incident. Therefore, agencies should follow agency-specific guidance and work to establish accounts in those systems for which their employees would routinely need access to content. Ideally implementing a federated ICAM solution is desirable to establish trust between the data provider and the end user organizations. For example, public safety personnel working in emergency communications centers might follow credentialing guidance from the NG911 Interoperability Oversight Council (www.ng911ioc.org). Access to those systems would involve the use of such protocols as ICAM (Identity, Credential, and Access Management), SSO (Single Sign On), bio metrics (e.g., facial recognition, fingerprint, etc.) and others. Ideally, a use of one or some combination of these methods should be established to ease the requirement for the end user to have multiple usernames and passwords across different systems. This is entirely possible, but not without careful planning of the identity management aspect of this ISF.

- **Data Exchange** – If the important data/content to achieve the mission has been identified, and access to that data has been granted, then the actual exchange of data needs to occur. This step involves the integration layer reaching into the data layer and exchanging the appropriate, timely content in a secure manner for the authorized requestor. The method in which the data will be exchanged depends on if it is in the right format for consumption by the end user in the presentation layer. More often than not, it

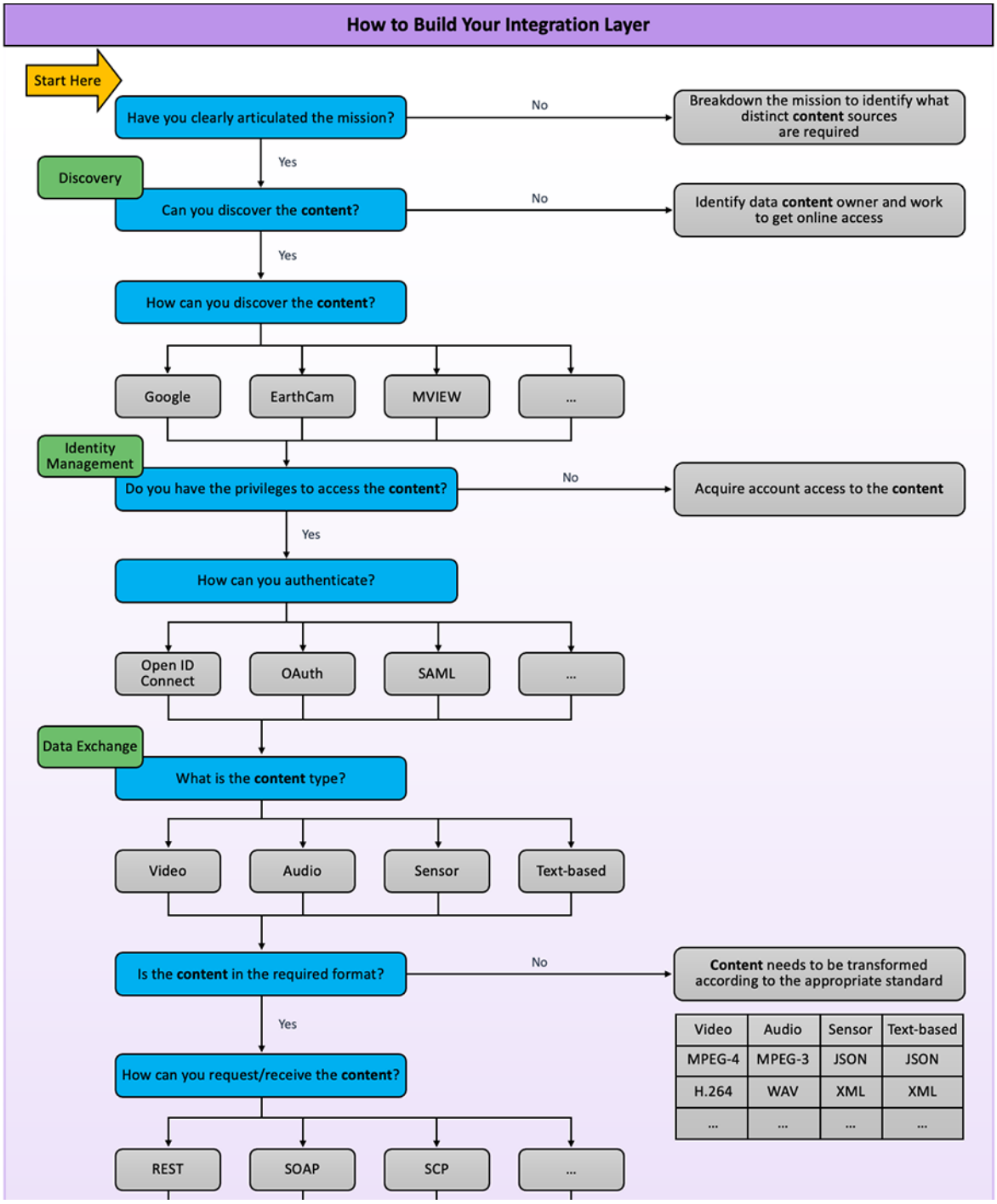
will not be in a readily consumable format, and thus the integration layer needs to reformat the information. This exchange and reformatting will be governed largely by three factors: the content itself, the standards that apply to that content, and the interface that is appropriate to that content. To return to a video example, MPEG 4 or H264 are standards that apply to video content. They are not applicable to LMR voice content, for which Project 25 (P25) may be the appropriate standard. The content determines which standard applies in the data exchange as it will drive the data formatting. Similarly, the appropriate interface (i.e. Application Programming Interface [API]) will depend upon the content and the application used in the presentation layer. REST, JSON, SOAP, XML are all interface formats/structures that are most applicable to different data content (see Appendix A for a further discussion of each of these interfaces). Thus, the actual data exchange will have to be tailored to the right standards and interface format that is appropriate for the needed content.

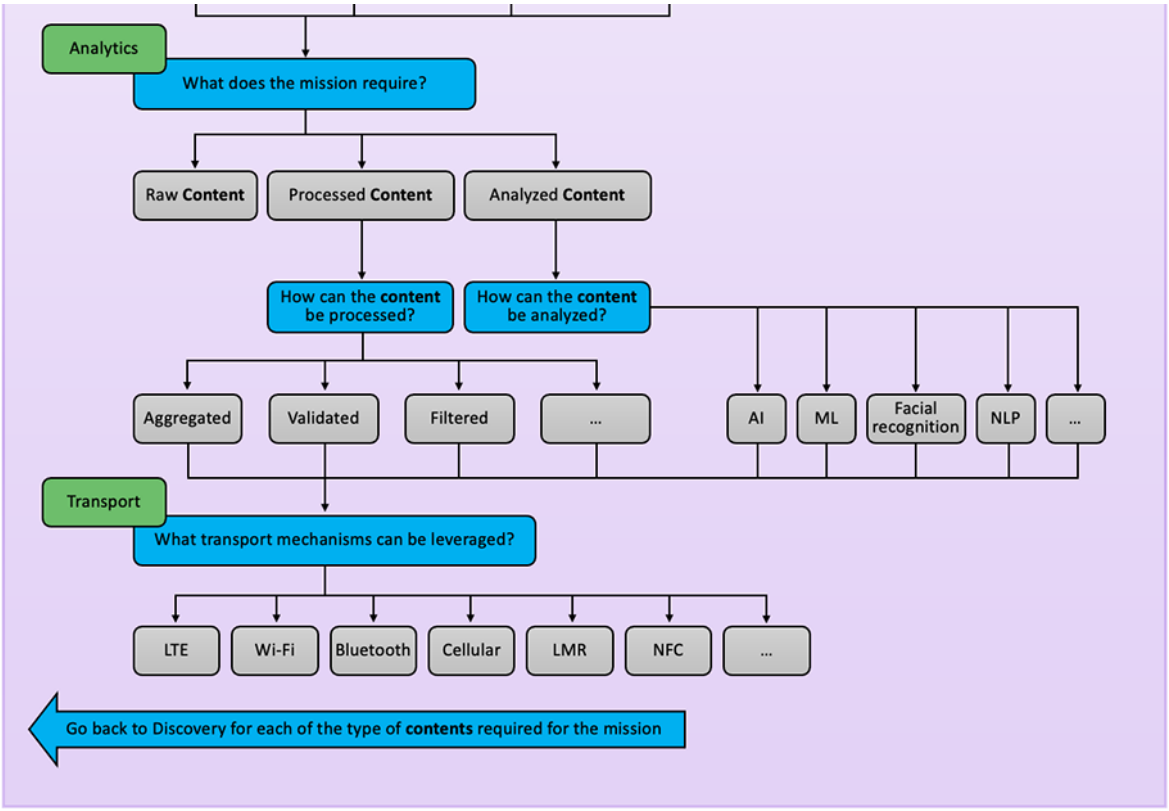
- **Transport** – The transport function occurs between the data and presentation layers and the integration layer. Transport is involved in accessing the data where it is originally housed and maintained as well as between the integration layer and the presentation layer where the end user will access and utilize the information. Transport is an important consideration because it will also impose certain formatting, bandwidth, and throughput constraints depending upon the content being transported. Transport could occur over near field communication, Bluetooth, WIFI, LTE, Satellite, Fiber, or Datacasting (i.e. television broadcast). In many cases, a number of these transport technologies may be employed in the movement of the information. Again, the content will have a bearing on the transport parameters. To continue with a video example, wireless transport of full motion, hi-definition video content wirelessly can be challenging. There may have to be tradeoffs in frame rate and quality to accommodate the bandwidth that is available. And such tradeoffs may require additional processing during the data exchange in the integration layer.

Before turning our attention to the Analytics function in the Integration layer, it is important to note that the previously discussed functions of the Integration Layer of Discovery, Identity Management, Data Exchange, and Transport should be common. The methods to perform each of these functions should be standardized within the ISF using widely accepted standards, tools, and techniques. While there needs to be appropriate security protocols overlaid on these functions, there should be nothing inherently proprietary about discovering, accessing, exchanging, and moving/transporting the needed data content. The basic decision to share information or not is found in the people and process aspects of interoperability, not the technology itself. (see the Executive Summary and Figure ES-2 for a discussion of people/process/technology). Individual technologies need to build in methods of sharing basic data across systems for the benefit of public safety, and public safety users should require this level of interoperability in their procurements. There is, however, a role for proprietary methods when truly unique intellectual property is involved. Within the ISF framework, it is believed that the more custom features of information sharing will be found in the Analytics function.

- **Analytics** – As more content is accessed in the data layer, aggregated, put in context, and shared as information to the Presentation Layer, some level of analytics will have to be applied. Without such analytics, there could be a tendency to provide to the end user an overwhelming amount of information, much of which may be irrelevant or even wrong. In various DHS-sponsored experiments involving data sharing to date, it has become clear that some form of adjudication is needed in order to send the right information to the right person at the right time. Today, that adjudication is performed by humans at ECCs such as Public Safety Answering Points (PSAPs), TOCs, EOCs, Fusion Centers, etc.

The graphic below illustrates a decision tree of how a public safety agency would progress through the integration functions discussed above.


How to Build Your Integration Layer
Start Here
Have you clearly articulated the mission?
No
Breakdown the mission to identify what distinct content sources are required
Yes
Discovery
Can you discover the content?
No
Identify data content owner and work to get online access
Yes
How can you discover the content?
Google
EarthCam
MVIEW
...
Identity Management
Do you have the privileges to access the content?
No
Acquire account access to the content
Yes
How can you authenticate?
Open ID Connect
OAuth
SAML
...
Data Exchange
What is the content type?
Video
Audio
Sensor
Text-based
Is the content in the required format?
No
Content needs to be transformed according to the appropriate standard
Yes
How can you request/receive the content?
REST
SOAP
SCP
...
Video
Audio
Sensor
Text-based
MPEG-4
MPEG-3
JSON
JSON
H.264
WAV
XML
XML
...
...
...
...



Key:	
Raw **Content**	Data that is unmodified from its data source. Transporting raw data means that consumers of that data have increased flexibility for analysis however, it will require much higher requirements for data transmissions rates and bandwidth.
Processed **Content**	Data that have been either filtered or reformatted. This can reduce the amount of data transmitted and can also helped to standardize transported data formats.
Analyzed **Content**	Data output of custom developed algorithms intended to identify specific items, objects, or subsets of data from the larger set of data.
NLP	Natural Language Processing – Branch of artificial intelligence that deals with the interaction between computers and humans using the natural language.
AI	Artificial Intelligence – the broad discipline of creating intelligent machines.
ML	Machine Learning – refers to systems that can learn from experience.
LMR	Land Mobile Radio – is a person-to-person voice communication system consisting of two-way radio transceivers.
NFC	Near Field Communications – is a set of communication protocols for communication between two electronic devices over a distance of 4 cm or less.
REST	Representational state transfer (REST) is a software architectural style that defines a set of constraints to be used for creating Web services. Web services that conform to the REST architectural style, called *RESTful* Web services, provide interoperability between computer systems on the Internet.
SOAP	Simple Object Access Protocol – is a messaging protocol specification for exchanging structured information in the implementation of web services in computer networks.
SCP	Secure Copy Protocol – command-line utility that allows you to securely copy files and directories between two locations.

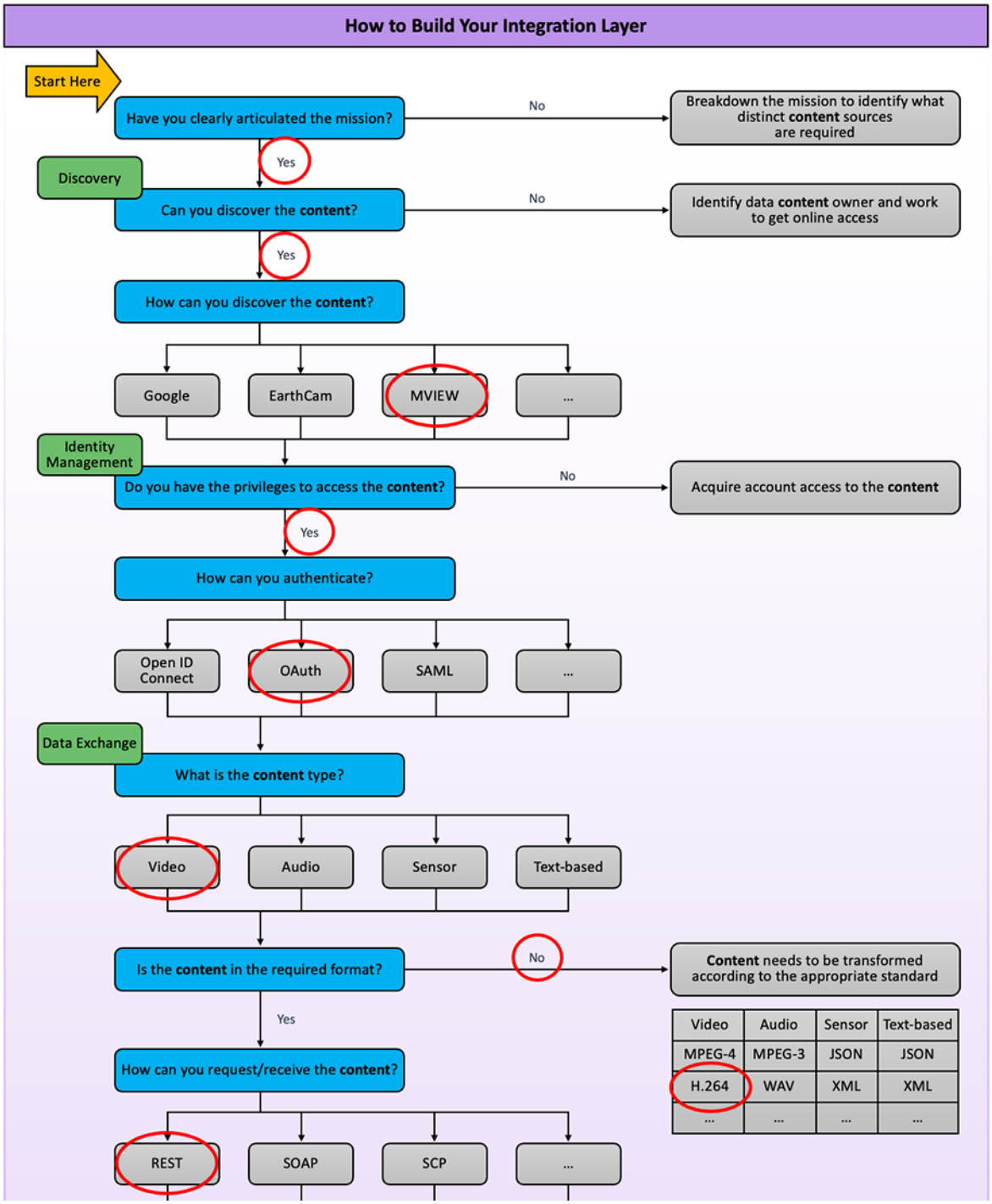
Figure 4-10: How to Build Your Integration Layer

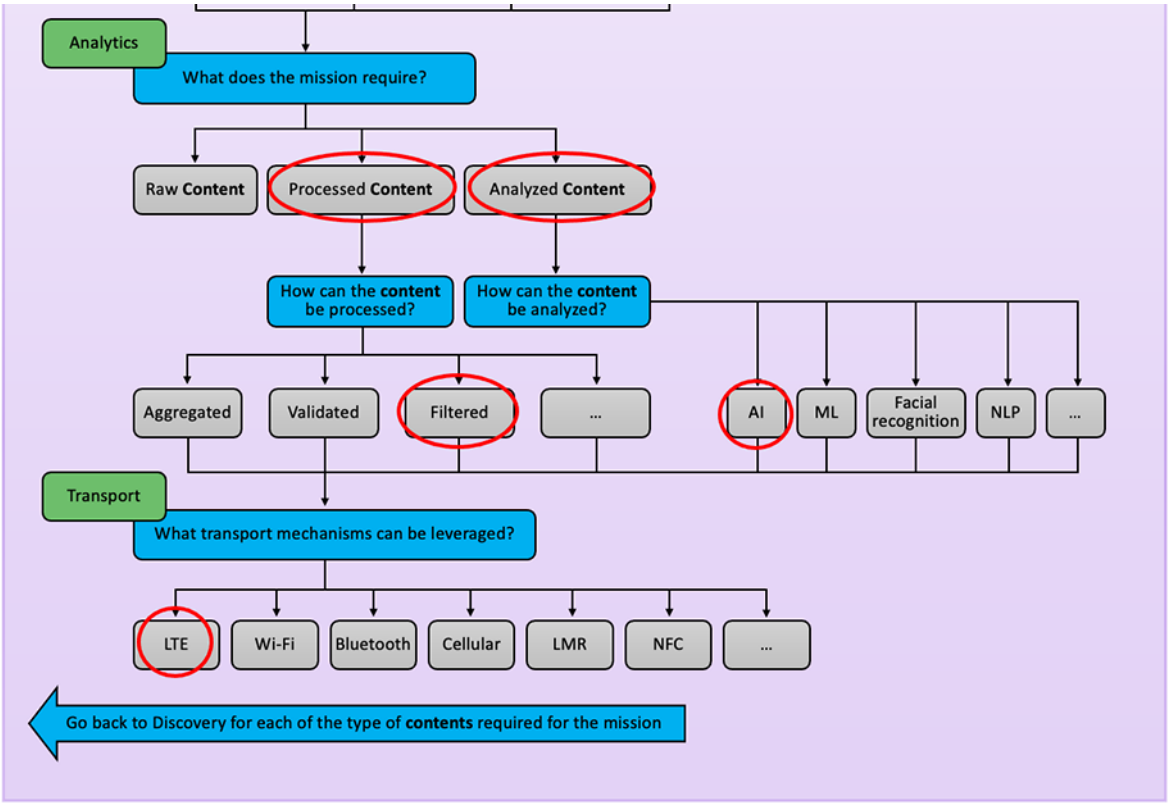
The previous diagram can apply to a particular mission and be used to better understand how to build the Integration Layer for a particular instantiation of the ISF.

For example, law enforcement may need to obtain video at the intersection where a pedestrian was struck. Further, they would need to be able to identify the vehicle and read the license plate. Applying the questions in the figure would require the officer, via his smart phone, to:

- Discover who owns the camera on the traffic signal pole (presume that it is the Department of Transportation)
- Gain access to that data layer system (presume the officer's agency participates in a regional GIS-based video sharing effort and the officer has rights in that system)
- Request the video from 30 minutes earlier
- Reformat the video content according to H264 standard via an API
- Process the video to parse out the prior 30 minutes of footage and analyze to detect when a person was struck
- Transport the roughly 30 seconds of video to a presentation layer application on the officer's smart phone for their evaluation

In walking through this example (see Figure 4-11), an IT specialist could begin to identify and put in place the necessary integration layer systems/applications, approval mechanisms, data conversions, analytics, and transport to accommodate the mission requirements.


How to Build Your Integration Layer
Start Here
Have you clearly articulated the mission?
No
Breakdown the mission to identify what distinct content sources are required
Yes
Discovery
Can you discover the content?
No
Identify data content owner and work to get online access
Yes
How can you discover the content?
Google
EarthCam
MVIEW
...
Identity Management
Do you have the privileges to access the content?
No
Acquire account access to the content
Yes
How can you authenticate?
Open ID Connect
OAuth
SAML
...
Data Exchange
What is the content type?
Video
Audio
Sensor
Text-based
Is the content in the required format?
No
Content needs to be transformed according to the appropriate standard
Yes
How can you request/receive the content?
REST
SOAP
SCP
...
Video
Audio
Sensor
Text-based
MPEG-4
MPEG-3
JSON
JSON
H.264
WAV
XML
XML
...
...
...
...



Key:	
Raw **Content**	Data that is unmodified from its data source. Transporting raw data means that consumers of that data have increased flexibility for analysis however, it will require much higher requirements for data transmissions rates and bandwidth.
Processed **Content**	Data that have been either filtered or reformatted. This can reduce the amount of data transmitted and can also helped to standardize transported data formats.
Analyzed **Content**	Data output of custom developed algorithms intended to identify specific items, objects, or subsets of data from the larger set of data.
NLP	Natural Language Processing – Branch of artificial intelligence that deals with the interaction between computers and humans using the natural language.
AI	Artificial Intelligence – the broad discipline of creating intelligent machines.
ML	Machine Learning – refers to systems that can learn from experience.
LMR	Land Mobile Radio – is a person-to-person voice communication system consisting of two-way radio transceivers.
NFC	Near Field Communications – is a set of communication protocols for communication between two electronic devices over a distance of 4 cm or less.
REST	Representational state transfer (REST) is a software architectural style that defines a set of constraints to be used for creating Web services. Web services that conform to the REST architectural style, called *RESTful* Web services, provide interoperability between computer systems on the Internet.
SOAP	Simple Object Access Protocol – is a messaging protocol specification for exchanging structured information in the implementation of web services in computer networks.
SCP	Secure Copy Protocol – command-line utility that allows you to securely copy files and directories between two locations.

Figure 4-11: How to Build Your Integration Layer Example

4.9 ISF COMPONENTS: FLEXIBILITY AND SCALABILITY

Emergency communications systems have been moving toward architectures that support greater levels of modularity and scalability. Advanced architectures have emerged that readily facilitate the generation of APIs that enable applications to interoperate without requiring changes to core functionality.

An underlying assumption is that as data interoperability improves and the ability to acquire and transport information increases, there will be an increasing need to curate that data to ensure first responders are not inundated with redundant, invalid, or useless information. The ISF can be used to enable data consumers to more easily integrate applications to curate data. Figure 0-12 below depicts how a modular architecture might be applied to achieve this. This functionality could be implemented in a highly centralized manner with the functions performed by a single system or application, or in a more distributed manner with each application hosted separately. The purpose is not to dictate how an agency will process its data, but rather to identify capabilities, structures, and best practices that will provide agencies with the flexibility to implement the functionalities they need. Although analytics are presented as part of the integration layer in the figures, there is a case to be made for their inclusion in the presentation layer as endpoint devices become smarter. In most cases, it is the end-user who requires control over the suite of analytics applied to an information stream in order to make the data most relevant to their particular mission.

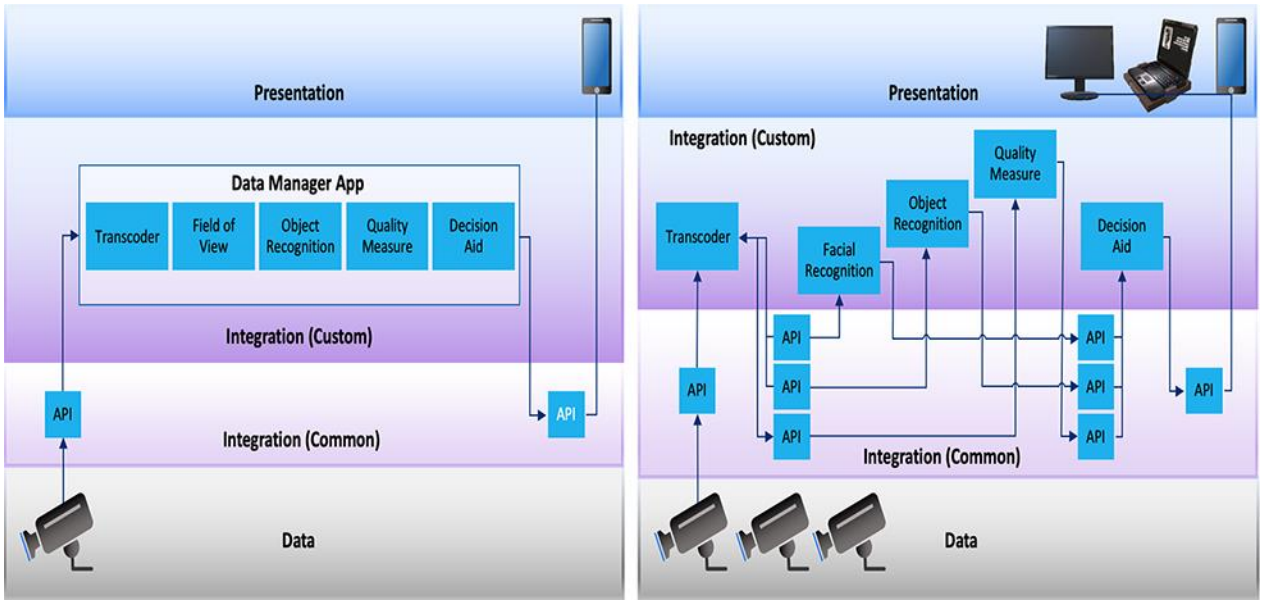


Figure 4-12: ISF Demonstrates Flexibility and Scalability

4.10 ISF Adoption and Implementation

As previously stated, organizations are continuing to invest in new products and technologies to improve their emergency communications and information sharing ecosystems. However, many of these new products and technologies force trade-offs among interoperability, flexibility, and sustainability, which impacts time to value for any agency. Investing in products and systems that inherently support wide-scale interoperability can minimize these trade-offs and enable a more rapid incorporation of any new product or capability into the existing operations.

Public safety organizations continue to struggle to find ways to integrate various products into emergency communications systems to support automation and enhanced capabilities. For example, if the one information technology (IT) person who custom scripted this integration departs for another job or decides to retire, the organization can rarely maintain existing functionality. This is a significant problem for organizations that have legacy systems, custom-developed products, or proprietary products and applications. Some public safety agencies have begun to focus on more timely and measurable return on investment (ROI) approaches. They are investing in products and applications that promote flexibility and interoperability, increasingly judging a product's worth by how often it is used and how many other solutions it connects with or supports.

The successful adoption and implementation of the ISF will require collaboration and coordination among product vendors, services providers, and product and service consumers. Interoperability requires public safety product vendors to converge towards standards so that their products can be more compatible with one another. If products continue to diversify in how they operate, interoperability will increasingly rely on custom integration hardware and software

components in order to achieve interoperability. However, customization is not the way to achieve universal interoperability because it is not a scalable approach. The community at large needs to understand how working together can have a multitude of benefits such as increased adoption and use of products that prioritize the use of standards. The use of standards will enable products to communicate and work in conjunction with other products and services.

A crucial component to the development of the ISF is engagement with the product vendors as well as the community that utilizes these products. By working together, they can better understand and characterize interoperability gaps, encourage vendors to fill those gaps, and ultimately help the public safety community meet their mission. Another activity that will help illuminate gaps in this space is the use of pilot activities to prove out concepts and demonstrate successful implementations of interoperability among disparate data sources.

Once the larger community has bought into the concept of interoperability, it will be up to public safety entities to employ ISF within their department or agency by making use of interoperable products and, when those aren't available, building scalable, extensible, and shareable integration components to fill their communication gaps.

Figure 0-13 below represents a notional workflow that could be used by a public safety entity to employ the ISF within their department or agency.

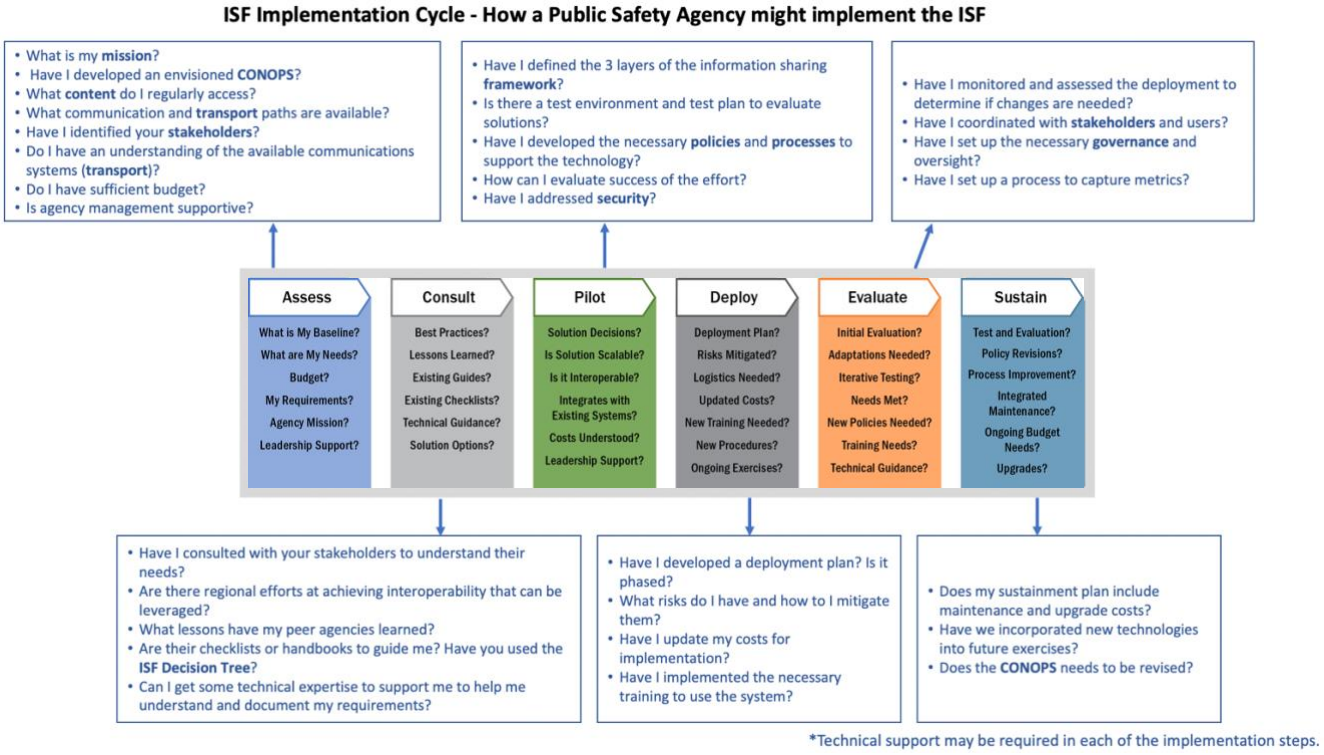


Figure 4-13: ISF Implementation Cycle

Within each step of the ISF Implementation Cycle there are a series of questions that the public safety agency or agencies should address before advancing to the next step. Appendix E includes a set of diagrams that provide a more detailed overview of each of the steps, a set of questions to answer, tools and resources, and a checklist of activities to help them to advance to the next step.

5 SUMMARY

In the first phase of this project, the problem of interoperability in the public safety space was described and included narrative of how the nature of an incident and its scale of complexity requires greater cooperation and interoperable communications between mutual aid responders. In addition, communications trends have brought other technology solutions to the information sharing and situational awareness toolbox such as license plate readers, body worn cameras, drones, dash cameras, and fixed security cameras as well as an ever-increasing number of datasets coming from a variety of sources. As the tools and data have multiplied, so have the transport paths that must carry the data from a point of origin (e.g., video camera) to a designated point of receipt (e.g., display monitor). The transport paths are also changing with personal communications now occurring over Bluetooth and Near Field Communications (NFC) systems, incident communications over Wi-Fi, and wide area communications using Broadband/Cellular 5G, satellite, and even television broadcast.

Thus, the public safety communications space is becoming increasingly complex with more and more data, tools, and transport pathways than ever before. This is both a welcome change as well as one that poses a number of challenges for end-users and operational personnel. While technology advancements bring new capabilities that are greatly needed, they also provide for a more complex data and information sharing environment that can be overwhelming for operational personnel. In addition, many of the existing legacy infrastructure in use in public safety today was not designed for the integration and interoperability of these advanced technologies and transport mechanisms.

To help fully understand the complexity of the current public safety information sharing environment, the first volume report introduced a three-layer construct as the baseline for a conceptual framework on how to approach these interoperability challenges. It introduced the *Data/Integration/Presentation layers* framework that could be used for designing a more interoperable collection of emerging and legacy technologies and transport systems. It is a pragmatic approach that accepts the fact that because these legacy systems were not designed using interoperability requirements, reconfiguring and updating these systems would entail enormous expense and added complexity (and possible system failures) that is unacceptable. However, advancements in technologies are providing more computing power than ever and the ability for public safety personnel to manage a multitude of data requires a more sophisticated and interoperable infrastructure for common situational awareness that supports sound decision-making needs during operational response.

Figure 5-1 depicts the critical role that interoperable information sharing systems will play for the future data integration expected from initiatives such as Smart Cities, Intelligent Highways, NG911 centers, and other sensors for analysis, control, dissemination, and enhanced decision support where the holy grail for public safety is to maintain near real-time situational awareness.

Figure 5-1: Depiction of Interoperable Information Sharing Systems

As described in this report, ownership of this data will be distributed across a range of entities and will need to integrate with future architectures that will:

- Allow for the rapid and flexible discovery of relevant data and data sources
- Support managing and exchanging identity and permissions securely, without burdening first responders and/or public safety personnel
- Enable data exchange and interoperable communications

This report provides a deeper dive into the integration layer and proposes a framework that both public safety practitioners and IT professionals and technology developers can use to design the detailed architecture needed to bring about greater interoperability. This report explains the five functions that need to be performed by the integration layer: *Discovery, Identity Management, Data Exchange, Analytics, and Transport*. Regardless of the data type, these functions will need to be performed to retrieve the data from where it customarily resides (in the data layer) to the end user (in the presentation layer) and then be transformed into consumable, actionable information. These tools and techniques vary depending upon the data type or content. The data standards that apply, formats, meta data, and transport paths all will have a bearing upon the ultimate IT architecture that must be designed between the systems; which is why this is such a hard problem. The ISF proposed in this report provides an approach and a number of aids to break down the complexity into its five component functions.

This report also provides an illustration of eight use cases selected to demonstrate how use cases can be broken down into steps that delineate the *mission, stakeholders, data content needed,* and *the transport paths* available, which then allows the technology professionals to begin to develop detailed requirements for the integration layer. Further, a decision tree is presented that walks the user through the thought process to select the needed IT tools (e.g, standards, exchange protocols, transport mechanisms) that are appropriate for the data that needs to be shared. If public safety stakeholders can identify an existing use case or use this tool to disassemble their specific use case(s), they will have a much greater understanding of their requirements and the necessary tools (technical and non-technical) required for achieving interoperability.

In order to achieve this, users must overcome the data interoperability challenge. As good as the private sector is at providing intellectual capital and creativity in addressing these public safety challenges, they are not necessarily incentivized to provide open architected, interoperable systems. Their approach is to provide a slice of the three layers (i.e. their hardware, software comprises the data/integration/presentation layers) which allows for a tightly integrated, optimized system with a good user experience. However, this design is not usually interoperable, which exacerbates

the problem. Furthermore, their business model and profitability are often linked to having customers rely on them to make, maintain, and update their systems.

If the market cannot provide for an increased interoperable public safety environment, then it can be argued that there is an essential role for government to play. While government cannot (and should not) dictate technology development, they can create a *framework* for public safety stakeholders to use to help them achieve an interoperable system. They can promote *standards* on how data can be published and consumed, guidance on how to *make data sets available* for public safety consumption, and support some of the *legal and IT security groundwork* to ensure those data sets are used as intended. They can promote standardized systems that *authenticate* the individual to provide secure systems, but avoid multiple login requirements. Most importantly, government partners can provide *training* on how to apply the principles in this report so that public safety practitioners and the technology community can have a common approach to the interoperability problem.

In summary, this report and its appendices provide an overarching construct that public safety can utilize to bring about greater interoperability. It provides the bridge between public safety practitioners, IT professionals, and technology developers, who often have very different perspectives. While there are various systems in place to provide situational awareness (e.g., video feeds, sensors, voice, text, etc.), comprehensive situational awareness does not come from any one data set. Therefore, these various systems must come together to derive awareness and understanding to support real-time decision-making needs. There are examples of systems that were built according to these principles that can be highlighted as effective practices, and many segments of the public safety community have current initiatives to improve interoperability. Those efforts can be supported and unified by also utilizing this framework. As the public safety community implements NG911, public safety broadband, and expanded use of video and sensors, we have the opportunity to promote and achieve greater interoperability through widespread use of this framework, instead of introducing yet more technologies, data, and complexity that will likely overwhelm public safety decision-makers and stakeholders.

Appendix A BASELINE TECHNOLOGICAL ASSESSMENT

Appendix A presents the results of a baseline technological assessment of emerging technologies and best practices and is a relatively technical appendix *intended for readers who are interested in a deeper understanding of the technological aspects relevant to achieving interoperability*. It includes discussion of several aspects of the technology-related components and their implications with respect to interoperability. This appendix is organized as follows:

1. **Application Program Interfaces (API):** Discusses Application Programming Languages (APLs) that will be foundational to enabling the functionality.
2. **Data Implications:** Delineates the most commonly used data for supporting public safety operations.
3. **Voice Implications:** Discusses the interoperability challenges present in voice communications.
4. **Identity Control Access Management (ICAM) Implications:** Presents an initial discussion of the security and credentialing mechanisms necessary for the enabling of data interoperability in public safety operations.
5. **Emergency Communication Centers (ECCs)** and **Next Generation 911** capabilities.

A.1 APPLICATION PROGRAMMING INTERFACES

One common mechanism for enhancing the modularity of an architecture is through the use of an API. An API is a communication protocol used to facilitate the integration of two applications in a client and server relationship. APIs define how a client can interact and make requests from a server. It is common to describe an API as a contract. The owner of content or a service (i.e. the server) guarantees delivery of a specific type of information in a specific format upon receipt of a specifically formatted query from the client applications. APIs enable developers to construct interfaces without affecting the core functionality of the application.

An API can be made public or kept private, depending on its purpose. Public APIs provide a means for anyone to access a particular server's data or services. Companies such as Google provide multiple different public APIs so that clients can make use of their various tools like Google Calendar and Google Drive. Using the public API, the developer of a third-party website could implement an interface to enable clients to access these services without requiring the clients to manually create the required interfaces. Private APIs are used to limit access. These APIs typically provide more capability to the user as they are only available to internal developers. For public safety, it will likely be desirable to develop limited access public APIs to enable relatively ubiquitous access across the public safety community and to limit access by those outside of public safety.

A.1.1 REST API

Representational State Transfer (REST)[2] is a software architecture for web services that defines constraints for interactions between services. This architecture has been commonly applied to APIs that act as a messenger for clients to engage with a server's data, allowing them to request and modify data using predefined stateless operations. REST APIs interact with servers by utilizing endpoints, known commonly as Uniform Resource Locators (URL's)[3] which are predefined by the REST API developer. Being a software architecture, REST does not define its own protocol but rather utilizes existing protocols. For example, the HyperText Transfer Protocol (HTTP)[4] implements GET, POST, PUT, and DELETE commands that are often used for data transactions with content being returned using data interchange

[2]Fielding R, 2000. REST: architectural styles and the design of network-based software architectures. Doctoral dissertation, University of California, Irvine, 2000.

[3]Berners-Lee T, Fielding R, and Masinter L, 2005. Uniform Resource Identifier (URI): Generic Syntax, RFC 3986, January 2005. Retrieved September 2019 from: ietf.org/rfc/rfc3986.txt

[4]Fielding R, Gettys J, Mogul J, Frystyk H, Masinter L, Leach P, Berners-Lee T, 1999. Hypertext Transfer Protocol – HTTP 1.1, RFC 2616, June 1999. Retrieved September 2019 from: tools.ietf.org/html/rfc2616

formats like JavaScript Object Notation (JSON)[5] or eXtensible Markup Language (XML).[6] For public safety applications, it may be desirable to use the Emergency Data Exchange Language (EDXL).[7] This flexibility enables REST to work as a well-defined broker between a variety of different systems.

For an API to be truly RESTful, it must meet the six REST architectural constraints. These constraints are:[8]

1. **Client-Server**: Clients and servers should be separated. This allows for clients and servers to change on their own without impacting the other.
2. **Stateless**: Communication between client and server must be stateless, meaning each message contains all information needed to handle the request. Because of this, all context of the session state is kept by the client.
3. **Cache**: Responses to requests must be labeled as either cacheable or non-cacheable. Clients can reuse cacheable data to lower the amount of data needed for future requests. This improves the efficiency and scalability of the system.
4. **Uniform Interface**: Resources should have a uniform interface that provides access to consumers. Paths defined for resource access should follow a pattern, providing a logical way for clients to request data.
5. **Layered System**: The server may implement a hierarchical architecture, allowing it to work as an intermediary between the client and other servers. The client may request data such that the server must contact a separate server before returning the request to the client. With this implementation, the client is unable to tell if it is connected to the end server or a server in between.
6. **Code on Demand**: Servers may send executable code to be run on the client's machine.

These design constraints promote an API that is able to work efficiently, securely, and across many platforms. For this reason, REST has been widely implemented within the community, with companies such as Google, Amazon, eBay, and Yahoo all making use of it. For the application of public safety data interoperability, REST APIs are a natural choice. The client-server separation in a REST architecture allows both sides to evolve and change independently of one another while still being able to interact. Therefore, departments would be able to maintain interoperability without needing to notify other departments of upgrades and changes that occur. The stateless nature of REST transactions adds another layer of security by forcing the client's authentication to be validated with each request. This validation is often done using Open Authorization (OAUTH)[9] in which a third-party application is used to verify the client's identity to the resource owner. This method is enabled by REST's layered system.

REST also works independent of its implementation, unlike other APIs such as Simple Object Access Protocol (SOAP) APIs, meaning it can be easily integrated into preexisting systems. The REST API can be added to the systems that

---

[5] Bray T, 2017. The JavaScript Object Notation (JSON) Data Interchange Format. RFC 8259, December 2017. Retrieved September 2019 from: tools.ietf.org/html/rfc8259

[6] Bray T, Paoli J, Sperberg C, Maler E, Yergeau F, 2008. Extensible Markup Language (XML) 1.0 (Fifth Edition), November 2008. Retrieved September 2019 from: w3.org/TR/xml/

[7] DHS, 2019. Emergency Data Exchange Language Suite of Standards, DHS Science and Technology Directorate. Retrieved October 2019 from: dhs.gov/publication/emergency-data-exchange-language-suite-standards

[8] REST API Tutorial, 2019. REST Architectural Constraints. Retrieved September 2019 from: restfulapi.net/rest-architectural-constraints/

[9] Hardt D, 2012. The OAuth 2.0 Authorization Framework. RFC 6749, October 2012. Retrieved September 2019 from: tools.ietf.org/html/rfc6749

public safety agencies have in place without needing to change the underlying systems. The REST API would connect outside users to the data that resource owners provide.

A.1.2 REST vs. SOAP

SOAP[10] is a messaging protocol specification used to transfer data for web services. SOAP standardizes a format for data to be exchanged via HTML using XML to allow for communication independent of platform. Each XML message contains the following elements:

- Envelope – required element that defines the start and end of the message.
- Header – optional element that describes the contents of the message. This determines how the receiver will interpret the data.
- Body – required element containing the content of the message meant for the receiver.
- Fault – optional element containing information on errors that occurred when processing the message.

Being a protocol rather than an architecture, SOAP is more structured and has more overhead than REST. The benefits of this are that SOAP APIs are typically more secure because they are able to implement Web Services Security (WS-Security) while REST can only use SSL (Secure Socket Layer).[11] The downside is that they require more resources and can be harder to implement due to being less flexible. Clients can interact with REST APIs without having any prior knowledge of the API. SOAP APIs must provide their Web Service Description Language (WSDL).[12] which describes every aspect of service, to clients before any interaction can occur. This means that any time a change is made on the server side, clients must receive the updated WSDL or else they will be unable to use the API.[13]

A.2 Data Implications

Interoperability includes the ability to access data and services hosted across multiple agencies and jurisdictions. The integration layer facilitates the exchange of data and services between applications hosted on different agency computer systems, enabling those agencies to share a common situational awareness. While the integration layer does not provide actual access into other agencies' computer systems, it does enable authorized users to interact with those systems. It must also enable individual agencies to continue to use their existing systems when interacting with other agency systems instead of needing to adopt and purchase a new system for accessing other agencies' data.

In addition to supporting the exchange of data between content owners and consumers, the integration layer needs to include analytics critical to public safety situational awareness. Four types of data have been identified for deeper investigation of how analytics might be included in the integration layer. These data are unique either because they are analytic products or because their usefulness is greatly enhanced by analytics. These four types of data illustrate the need for an interoperability capability that supports the seamless integration of analytics. Specifically, public safety communications depend on the ability to move relevant data to and from the appropriate analytics engines:

---

[10] Box, Kakivaya, et al., 1999. SOAP: Simple Object Access Protocol. Internet Engineering Task Force (IETF) Tools, Sept. 1999. Retrieved October 2019 from: tools.ietf.org/html/draft-box-http-soap-00

[11] Guru99, 2019. Web Service(WS) Security Tutorial with SOAP Example. Retrieved October 2019 from: guru99.com/security-web-services.html

[12] Vocell J, 2019. A Beginner's Guide to SSL: What It Is & Why It Makes Your Website More Secure. Hubspot. Retrieved October 2019 from: blog.hubspot.com/marketing/what-is-ssl

[13] Wodehouse C, 2017. SOAP vs. REST: A Look at Two Different API Styles. Upwork. Retrieved October 2019 from: https://www.upwork.com/hiring/web-development/soap-vs-rest-comparing-two-apis/

- Geographic data from Geographic Information Systems (GIS)
- Video data
- Telemetry data from sensors
- Incident Management and Computer Aided Dispatch Data

A.2.1 GEOGRAPHIC DATA AND GIS

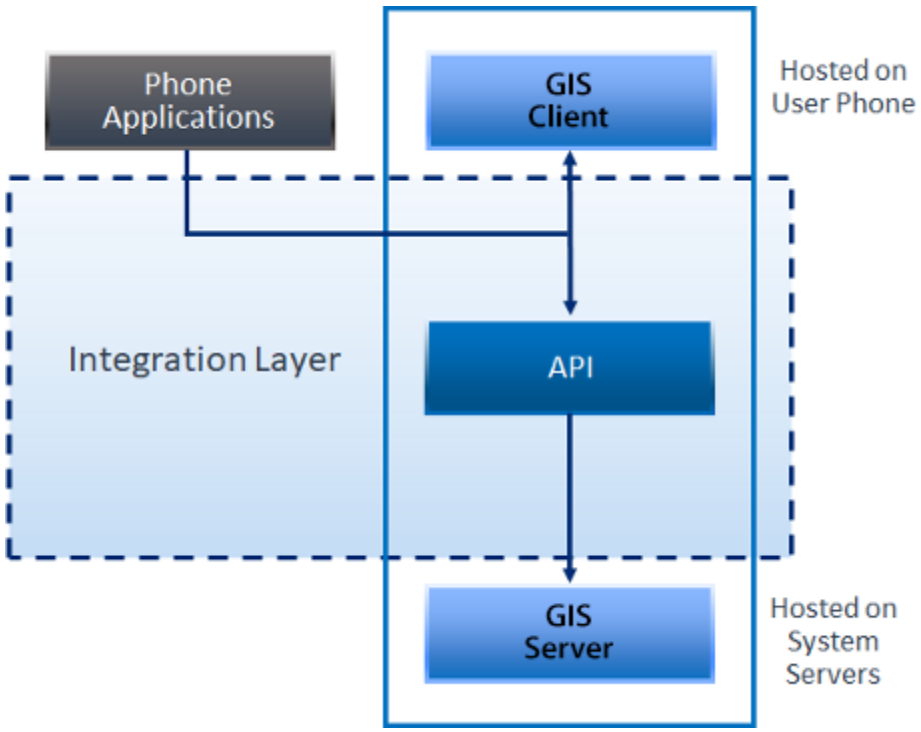
GIS is a computer system that captures, stores, checks, and displays information related to positions on the Earth's surface.[14] GIS can provide first responders with vital spatial and geographic data. GIS is a system for aggregating and analyzing data to improve situational awareness. GIS maintains stored geographical data -- including information about the location of resources, high value structures, or people – and applies sophisticated graphics capabilities to present information in a meaningful way across a wide range of platforms. Also, GIS normally includes analytics to enable users to derive additional levels of meaning from the available geographic and spatial data. Analytics can range from the simple navigation aids hosted on most smart phones to more sophisticated software packages used to support long-range planning by large corporations and public agencies.

In some cases, GIS information may also be useful to the public in the surrounding area (e.g., providing information regarding evacuation routes), and therefore many public safety entities have implemented GIS-based information sharing for public information emergency communication needs.

A.2.2 DATA PROFILE

In general, data required by a GIS application will reside in a system database. Instantiations of the GIS application will be hosted on various platforms and will communicate with system servers to receive required data and to execute desired algorithms when needed. The GIS application hosted on a smart phone may be little more than the software required to access the GIS system servers (or it may include rudimentary software to store and present maps downloaded from the system server). Apx Figure A-1 provides a high-level view of the distributed nature of a GIS application. In this figure, GIS applications refer not only to applications for manipulating geographic data, but also to the server applications that access and send the data and data products.

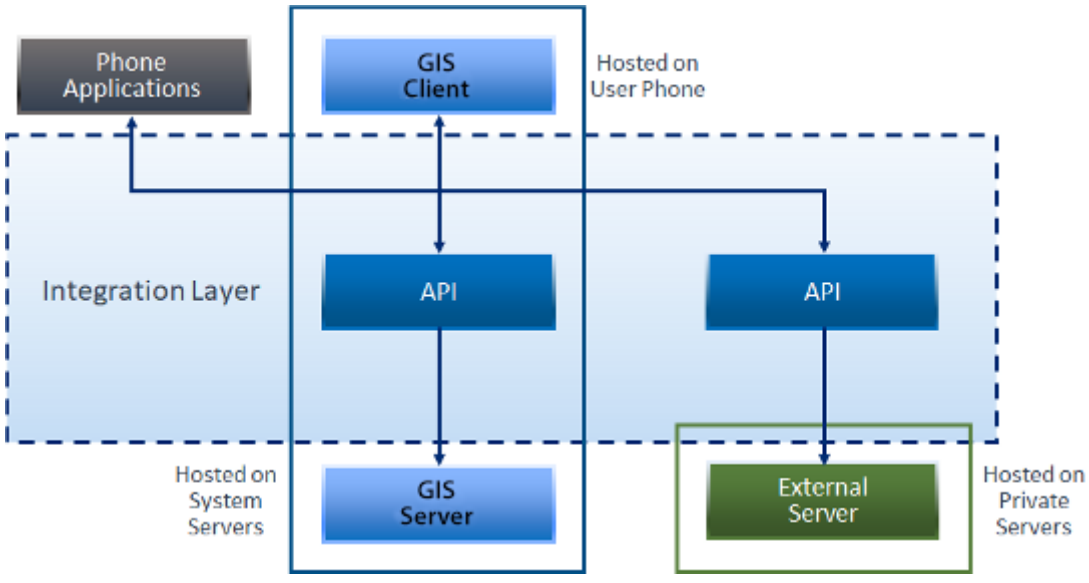
[14] National Ocean Service, "What is a geographic information system?" https://oceanservice.noaa.gov/facts/gis.html



Apx Figure A-1: Integration Layer View of GIS

In general, a GIS application will be implemented in a distributed fashion. A client application will reside on a host, such as a smart phone. It will have sufficient functionality to interact with the host platform and with GIS data bases via an API, as shown in Apx Figure A-1. It may also have some analytics to manipulate geographic data. In either case the functionality required to implement the API would be consistent with the model presented in Apx Figure A-1.

Apx Figure A-2 depicts the functionality needed to enable the client to interact with other databases via additional APIs.



Apx Figure A-2: Integration View of GIS with External Servers

A.2.3 DISCOVERABILITY

In order to perform its required functions, a GIS application must be able to locate services on the host platform (e.g., a platform's Global Positioning System for location information and its Internet services), its system servers, and any public or private databases to be used. Most commercial GIS applications include backend processing to enable access to information across a range of common commercial products, although end users may need to install a product compatible with the existing platform (e.g., the iOS or Android version of the application).

Similarly, GIS applications will need to be able to locate the system servers containing detailed mapping information and hosting more advanced decision support analytics. As both the application on the smart phone and those within the servers are owned by a common entity, the required location information is likely to be incorporated into the application backend.

Locating additional data sources, including public and private databases, will require additional discovery services. These can be as simple as provision of an Internet Protocol (IP) address or Uniform Resource Locator (URL) or may involve a more complex process including the exchange of metadata to enable the application to locate the required data source.

A.2.4 ACCESSIBILITY

Both the GIS system servers and the external database servers identified in Apx Figure A-1 and Apx Figure A-2 would limit access to authorized users. It is anticipated that the GIS servers have access controls to restrict access to their paid customers using their application and have safeguards against intrusion or use of their servers by others. Similarly, the external database content owner would require some form of identification before allowing access. The interface between the GIS application and the external database server would need to include the ability to provide and verify authorization information.

A.2.5 DATA EXCHANGE

Both the GIS servers and any external servers will need to provide data to the requesting application in an understandable format. In the case of the GIS servers, this is assumed to be a solved problem, as both the requesting application and the server will have the same developer. In the case of the external server, the application and the server would need to be able to exchange information, likely in the form of an API, to enable the external server to provide data in the appropriate format. Fortunately, there are standards[15] defined for exchange of geographic data.

A.2.6 VIDEO

As video surveillance systems have proliferated and the ability to move video streams has improved, the demand for video for both public safety and non-public safety applications has increased dramatically. According to a recent assessment by Cisco, video traffic accounted for three quarters of all IP traffic in 2017 and is projected to surpass 80% of IP traffic by 2022.[16] Video surveillance is expected to increase sevenfold during that same time period (although it will still represent only 3% of video IP traffic).[17]

---

[15] Federal Geographic Data Committee, 2019. Geospatial Standards. Retrieved October 2019 from: https://www.fgdc.gov/standards

[16] Cisco, 2019. Cisco Visual Networking Index: Forecast and Trends, 2017-2022 White Paper. 27 February 2019. Document ID 1551296909190103. Retrieved October 2019 from: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html

[17] JHU APL, 2015. Advanced communications video over LTE: efficient network utilization research, JHU APL Report AOS-15-1005 to the US Department of Homeland Security Science and Technology.

It has been demonstrated that if the appropriate video data can be provided to decision-making personnel in a timely manner, response operations and responder safety could both be improved. While the added capability of video data has been determined to be beneficial, there are also common concerns primarily in the areas of planning/procedures, as well as the technical and human resources required to manage video data. Public safety personnel provided feedback during video integration testing which included:

- Video data could help to align initial tactical decision making.
- Video data could enhance the recovery of injured persons in a timely manner when incident command (IC) can see victim locations in relationship to cleared or controlled threat areas. It would help in selection of entry points to achieve the maximum benefit (e.g., safety and timeliness of response) for emergency responders such as a Rescue Task Force (RTF).
- Information was shared between law/fire and EMS almost as soon as the video was connected. It was a great asset for unified command.
- To add video data for the purposes of enhanced decision-making, the mission needs and readiness levels of the public safety agency must first be well understood.
- Any time additional information is being added for the intended purpose of a first responder's situational awareness need, extensive consideration must be given to ensuring the right information is available at the right time for the right mission.
- First responder operations and related communications needs will continue to be a challenge when it involves processing large amounts of video for optimal results.

The following subsections address three aspects of the video data *set: 1) Data Profile, 2) Discoverability, and 3) Accessibility.*

A.2.7 Data Profile

Video can be either real-time video feeds from live cameras or recorded non-real-time video footage. There are many parameters associated with video data: the location of the camera, the format in which the video is captured, the compression algorithm used, video quality, the delivery mechanism, times of capture, etc. All of these parameters either influence or dictate how the video data can be utilized by a first responder. For example, the data may or may not have high enough resolution to deliver the information that the first responder seeks, the frame rate in frame per second (fps) may or may not be frequent enough, the overall quality may be too poor, the times when video was captured may not be inside the window of interest, etc. The following is a non-inclusive list of camera parameters that will influence the usefulness of any video data captured relative to first responder needs:

- Owner
  - Government agency
  - Private sector
  - Public sector
- Address
- Location (latitude, longitude, height above ground level)
- Mounting location (head, shoulders, chest)
- Accessibility
  - Available on the network
  - Request to owner
  - Physical visit
- Siting (elevation, azimuth)
  - Fixed
- Direction
  - Adjustable
- Direction range

- Field of view (h° x w°)
  - Fixed via prime lens
  - Variable via zoom lens
- Times of operation
  - Always on
  - Scheduled
  - Motion activated
- Mode of operation
  - Real-time feed
  - Stored data
- Historical length of stored data
- Sensor type
  - Color
  - Monochrome
  - Infrared
  - Other
- Resolution
- Frame rate
- Brightness
- Quality level
- Video Format (codec)
  - Standard
  - Proprietary

A.2.8 DISCOVERABILITY

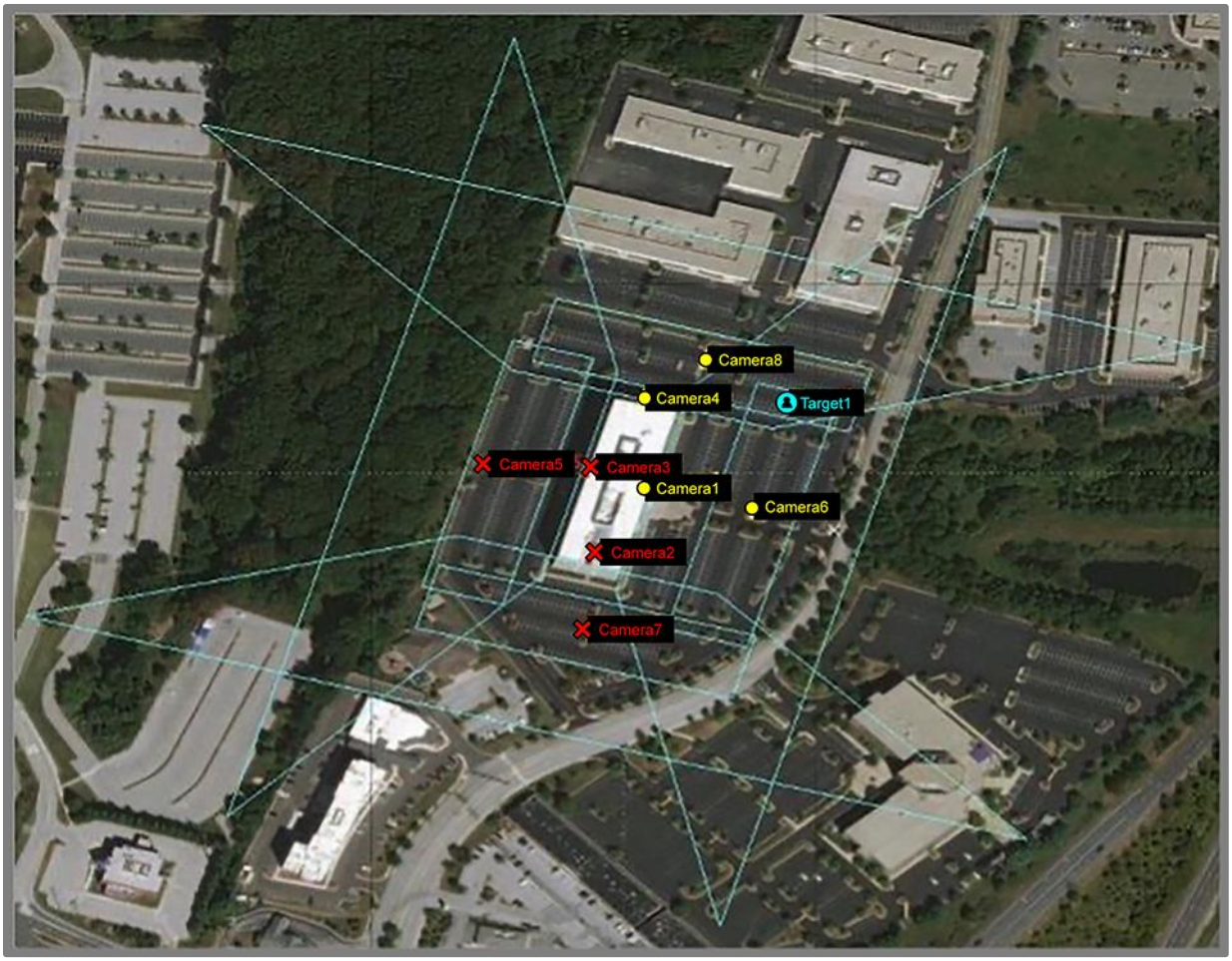
Accessing video data relevant and helpful to a mission can be a challenge. For example, as of 2014, there were 125 surveillance cameras per person in the United States.[18] Identifying which of these cameras have a view of an incident scene that can provide an image of sufficient quality to enhance situational awareness is currently not feasible as the responders' decision-making requirement is for timely and accurate information. Apx Figure A-3 illustrates a notional example of a building complex with a number of cameras providing differing fields of view. In this particular example, Target 1 is visible to cameras 1, 4, 6, and 8; the other cameras are unable to capture the target due to obstructions. An integration layer could make cameras 1, 4, 6, and 8 discoverable to first responders responding to this hypothetical incident. A set of analytics that could further provide an assessment as to which of the four potentially redundant views provided the most relevant and useable information may also be required.

In most cases, responders will not be interfacing directly with individual cameras, but with the server that controls them; thus, the problem will often be how to discover the video surveillance systems controlling the cameras with the view needed to support response to a specific incident. Video surveillance systems that integrate with advanced decision support tools will be required in order to be useful.

Additionally, real-time imagery from video cameras integrated into other Internet of Things (IoT) devices such as personal phones and other mobile devices can also provide valuable information. Video content has also become available through social media platforms and other mobile applications. Therefore, the discoverability of video goes beyond just identifying the traditional video control system and includes discovering video from personal IoT devices as well as already online video utilized for mobile and social media applications.

---

[18] Statista Research Department, 2018. Number of surveillance cameras per thousand people in the US, UK, and China 2014. Retrieved October 2019 from: https://www.statista.com/statistics/484956/number-of-surveillance-cameras-per-thousand-people-by-country/



Apx Figure A-3: Notional Map of Video Camera Locations and Fields of View Relative to a Target

A.2.9 Accessibility

A critical aspect of video is ownership of the data, which typically falls into one of the three use cases:

1. Public safety agency A owns its own data and needs to access it
2. Public safety agency B owns the data that public safety agency A needs to access
3. Private sector entity owns the data that public safety agency A needs to access

Challenges associated with the first use-case (1) are typically related to technical requirements. The public safety entity consumer of the video data would need only provide proof of the consumer's identity as a member of the public safety agency to access the data.

The second (2) and third (3) use-cases require providing a public safety agency access to third party data. In both cases, the conditions under which video data could be received, who would be allowed to view it, and even how the video might be used, requires negotiation between the public safety agency and the content owner. It is likely that there will be privacy and other policy issues, especially if it involves the law enforcement community. In addition, data storage, the ability to verify its authenticity, chain of custody, and other characteristics will require consideration.

A.2.10 Data Exchange

As with any other data exchange, the application receiving the video data and the application requesting and transmitting it will need to be able format and stream the data in a pre-arranged compatible format. When the video

transfer occurs within a single agency, formats will likely be readily understood without any additional processing. However, even in this case, the requesting application may need to specify features of the video including potentially frame rate, resolution, field of view, and other quality of service-related parameters. When the video is owned by a third party, additional processing may need to be applied. For older systems, the format and delivery mechanism may not follow Internet standards. Transcoding from a non-standard video format to a standard video format decodable by the first responders' viewing apparatus may be required.

As noted previously, the consumption costs associated with viewing video – i.e., the time required by a first responder to watch a video and interpret the information within it – are relatively high. Video streams may be subjected to analytics to assess redundancy, video and audio quality, and even relevance of the contents prior to dissemination to first responders. Technologies such as artificial intelligence and advanced image processing can be utilized to sort, filter, and refine the data before it is even presented to the first responders as relevant information.

A.3 Sensor Technology

The advances in sensor technology over the past two decades have sparked a proliferation of sensor deployment in a wide variety of user communities including the military, consumer, industry, and public safety. Furthermore, advances in communications networks and technologies such as the IoT and fifth generation (5G) cellular technology promise a dramatically increasing connected world of sensors. Thus, there will be an expansion of the volume of data in the Data Layer that is consumable by users in the Presentation Layer. This motivates the development of advanced techniques in the Integration Layer to maximize the advantages of data collected from sensor technology.

A.3.1 Data Profile

The public safety community would highly benefit from access to data collected by sensors of different types of configurations and modalities.

Sensor technology that is deployed by the public safety community itself includes wearables such body-worn cameras or other body-worn sensors that can perform real-time monitoring and alerting for health and environmental conditions. The data from these sensors provide a picture of the first responder's real-time experience. The public safety community also deploys their own sensors within the community. For example, video cameras may monitor critical parts of a community, and smoke alarms or carbon monoxide detectors provide alerting of fire-based or other hazardous incidents. The Integration Layer will need to facilitate access to a range of sensors belonging to local, state and federal government agencies and commercial entities including utilities, universities, hospitals, and others.

While there are sensors deployed/owned by the public safety community itself, there are also those deployed by private citizens either for personal or commercial use. Advancements in sensor technology has brought easier acquisition and deployment of sensors of a wide variety of modalities. One of the most common sensor modalities is that of video cameras. Furthermore, there are a plethora of other modalities in commonly deployed sensors such as imagery, acoustic, radio frequency (RF), temperature, atmospheric, and Global Positioning Systems (GPS). Smart homes and smart cities with a wide variety of interconnected sensors as part of the IoT infrastructure can provide first responders with an enriched picture as they respond and work through an incident.

A.3.2 Discoverability

In order to leverage sensor technology to its fullest extent during an incident response, the public safety community must have a means by which to discover sensors with relevant information. As with cameras, interactions will be between public safety systems and monitoring systems operating the sensors. This challenge mirrors closely that presented with respect to cameras in the previous section.

A.3.3 Accessibility

Upon discovery of a given relevant sensor, public safety personnel must be able to gain access to the data. If first responders are to fully leverage the emerging 5G enabled IoT, they will need to be able to access cameras not belonging to public safety or government. Use cases associated with integration of 5G IoT capabilities with public safety

communications call for public safety to be able to access a host of 5G enabled devices – thermostats, sensors, alarm systems – to provide public safety officers with more comprehensive situational awareness before entering buildings or other potentially dangerous environments.

As with cameras, this will require access to third party data. In most cases, the accessed information will be less sensitive and arguably less intrusive than video, such as thermostats and smoke alarms. However, medical data is one class of telemetry data that may be deemed even more sensitive. Use cases have been proposed in which first responders have to enter the homes of ailing persons whose medical status is being monitored. In some of those use cases, access to that medical information can be lifesaving. Terms of service for systems holding potentially life-saving data should define the conditions when that data may be accessed, who may access the data, how the data may be used, and what proof of access is required to protect against unauthorized disclosures.

Personal Area Networks comprised of 5G enabled devices will present a similar dilemma. Biometric sensors can provide timely warnings of first responders under stress but achieving this level of protection requires collection of sensitive private information. Accessing this private information introduces privacy related challenges and concerns. While not explicitly a technical problem, public safety agencies hoping to leverage the increased potential of 5G enabled technology to protect first responders will need to reach agreements with their officers before the collection of data.

Once the data from relevant sensors has been collected, employment of methods and techniques such as sensor data fusion or other algorithmic techniques can enable powerful and enriched understanding of the environment surrounding an incident and how best to deploy resources for incident response. Depending on the scale and severity of the incident, this discoverability, accessibility, and data processing workflow must be able to take place in real time. There are many research communities that are developing techniques to enable rapid decision-making using multi-modal and multi-layered approaches to fusion of sensor data. These techniques will play a critical role moving forward in the public safety community's ability to fully leverage the capabilities of sensor technology.

A.4 Incident Management Systems/Computer Aided Dispatch

Incident Management Systems (IMS) and Computer Aided Dispatch (CAD) systems are top-level tools that enable first responders and the public safety community to execute coordinated responses to incidents. Both systems support monitoring of on-going incidents and resource allocations. CAD systems are installed in ECCs. When a call for help is received, a CAD system supports information management needs and resources. In contrast, an IMS, like the National Incident Management System (NIMS) deployed by the Federal Emergency Management Agency (FEMA), provides a more enterprise set of capabilities designed not only to support incident command and dispatch, but to provide functionality to first responders at all levels of incident response.

A.4.1 Data Profile

IMS and CAD systems are intended to enhance situational awareness. Both systems depend on data entry by dispatch and have the ability to monitor resource usage. CAD systems also have the ability to provide an interface to personnel in the field, including personnel in vehicles.

A.4.2 Discoverability

Discoverability is not generally an issue because both IMS and CAD systems are highly centralized with a known address on the Internet.

A.4.3 Accessibility

Access to both a CAD system and an IMS system, as well as data from these systems, is highly controlled. Read and Write will have different levels of access. In general, only authorized users will have permission to input to a CAD or IMS database or to access data in these systems.

A.4.4 Data Exchange

Interoperability between CAD systems is a known data sharing issue. First responders operating outside their home jurisdiction will need to be able to access information provided by different CAD systems.

A.5 Voice Implications

A.5.1 Land Mobile Radio

Land mobile radio (LMR) is a terrestrial communications system that supports wireless push-to-talk technology for operating portable or mobile radio units, such as walkie-talkies or digital radios, on person or in vehicles.[19] The communications system consists of two-way transceivers, allowing for one-to-one and one-to-many voice calls.[20] Furthermore, LMR operates on frequency spectrum (VHF, UHF, 700 MHz, and 800 MHz bands) and at power levels (3 to 100 Watts) which offer favorable propagation characteristics for long-range communications. Currently, these characteristics make LMR the dominant form of voice communications for federal, state, local, tribal, and territorial first responders.

Two main types of LMR networks exist: conventional and trunked. Conventional LMR allows individual groups of users allocated dedicated frequencies and channels. When a user in a group selects a channel and makes a call, other members of the group cannot use the channel until the call is over. Trunked LMR systems dynamically allocate channels. When a member of group begins a call, an automated system searches for an available channel instead of the user manually selecting one. Both system networks are currently in use. Other potential variabilities in LMR exist because of the multitude of options for choosing standards and protocols. Therefore, various forms of LMR networks, with differences in interfaces, capabilities, and operation, have been developed by numerous organizations for private, commercial, and public safety applications.

Project 25 (P25) is a suite of LMR protocols and standards jointly developed by Association of Public-Safety Communications Officials (APCO), Telecommunications Industry Association (TIA), National Association of State Telecommunications Directors (NASTD), and National Communications System (NCS).[21] P25 defines specific capabilities, interfaces, and functions for a compliant LMR component, and thus eliminates disparate, non-interoperable public safety communications systems.[22] Conventional and trunked systems are supported by the standard. P25 is being deployed in three phases with enhanced functionally and spectrum utilization for each consecutive phase. New P25 radios are required to be backwards compatible with legacy radios in analog mode and previous legacy P25 radios in digital or analog mode. P25 standards provide interoperability mechanisms for connecting separate P25 LMR networks through the use of Radio Frequency Sub-Systems (RFSSs). The P25 standard was developed with public safety communications needs in mind and is publicly available to allow any manufacturer to produce their own compatible radios. A key downside of P25 LMR is the low-data rate. The maximum of 9600 bits/s makes video-sharing and data-sharing a slow process. Nevertheless, P25 radio has been accepted as the dominant

---

[19] Chaudhry, A.U. and Hafez, R.H., 2019. LMR and LTE for Public Safety in 700 MHz Spectrum. Wireless Communications and Mobile Computing, Volume 2019, Article ID 7810546, 17 pages. https://doi.org/10.1155/2019/7810546

[20] Powell J., 2012. Land Mobile Radio (LMR) 101. National Public Safety Telecommunications Council (NPSTC). Retrieved September 2019 from http://www.npstc.org/download.jsp?tableId=37&column=217&id=2489&file=LMR_101_NPSTC_Presentation_120725.pdf

[21] Daniels Electronics Ltd, 2004. P25 Systems Training Guide. Document TG-001-1-0-0, Daniels Electronics, Victoria, BC, Canada.

[22] Signals Analytics LLC, 2017. Mission Critical Push-To-Talk (MCPTT) Implementation for Colorado.

LMR protocol for public safety communications within the US at approximately 95% of market share across local, state, and national jurisdictions.[23]

A.5.2 Mission Critical Push-to-Talk (MC-PTT)

The 3GPP standards organization has specified mission critical push-to-talk (MCPTT) as part of long-term evolution (LTE) voice service.[24] MCPTT over LTE implements an enhanced push-to-talk (PTT) capability similar to LMR communication protocols on broadband LTE networks suitable for mission critical events.[25]

Groups and users are defined within the network and users can initiate one-to-one, group, and broadcast voice calls with floor control. Group management can be controlled dynamically. MCPTT provides modifications to the LTE protocol stack, such as the Group Communication System Enablers (GCSE) service, to support these services. GCSE are functions and interfaces that can be utilized to produce Group Communications Services. Group Communications support the transfer of data communications, including voice and video, to multiple users in a fast and controlled manner. GCSE for LTE will allow parallel communications between users and multiple groups (e.g., voice to one group, distinct streams of data to various other groups).[26]

Prioritization and resilience of MCPTT network traffic is implemented through the use of enhanced Quality of Service (QoS) bearers and Proximity Services (ProSe). QoS ensures a maximum latency time and guaranteed minimum bit rate. This is enabled by QoS Class Identifiers (QCI), which control the prioritization and scheduling of data throughout the network.[27] ProSe, or LTE-Direct (LTE-D), is currently being developed to work off-network to enable direct communications between mobile users or user equipment (UEs). Direct device to device communication saves network resources while enabling correspondence among first responders even in the absence of network infrastructure coverage.

A.5.3 Push-to-Talk over Cellular

Push-to-talk over cellular (PoC) emulates two-way LMR communication. It is a mobile telephony service for individual and group half-duplex communications over cellular. Recent broadband PoC telecommunications systems use LTE. PoC has two operating modes. In auto answer, recipients automatically hear the sender's voice, and in manual answer, recipients must actively accept the connection. Once in a call, floor control is a method for handling speaking priorities and privileges for all participants. Because PoC is available on a wide range of cellular devices, such as commercial

---

[23] Public Safety Technology Alliance, 2019. Land Mobile Radio (LMR)/Long Term Evolution (LTE) Interoperability Technical Subcommittee Report. Public Safety Technology Alliance (PSTA), Fremont, CA. Retrieved September 2019 from: https://www.pstalliance.org/technical-committees/subcommittee-report-and-comment-form/

[24] European Telecommunications Standards Institute, 2018. Technical Report LTE; Mission Critical Push to Talk (MCPTT) over LTE, Stage 1; (3GPP TS 22.179 version 15.2.0 Release 15). European Telecommunications Standards Institute (ETSI), ETSI TS 122 179 V15.2.0 (2018-07)

[25] National Public Safety Telecommunications Council, 2018. Public Safety Land Mobile Radio (LMR) Interoperability with LTE Mission Critical Push to Talk. National Public Safety Telecommunications Council (NPTSC). Final Report January 8, 2018. Retrieved September 2019 from: www.npstc.org/download.jsp?tableId=37&column=217&id=4031&file=NPSTC_Public_Safety_LMR_LTE_IO_Report_20180108.pdf

[26] European Telecommunications Standards Institute, 2014. Technical Report LTE; Group Communication System Enablers for LTE (GCSE_LTE); (3GPP TS 22.468 version 12.1.0 Release 12). European Telecommunications Standards Institute (ETSI), ETSI TS 122 468 V12.1.0 (2014-10)

[27] Signals Analytics LLC, 2017. Mission Critical Push-To-Talk (MCPTT) Implementation for Colorado.

and ruggedized smart phones, broadband PoC can augment existing LMR systems already embedded in various organizations. A complication of PoC is its non-interoperability between different vendors and/or carriers. For example, users on Sprint's PoC services cannot communicate with users on Verizon's PoC.[28]

A.5.4 Interoperability Issues and Proposed Solutions

Gaps in the interoperability of legacy LMR systems, specifically P25 systems, prevents first responders from seamlessly and effectively coordinating during incident responses which require multi-jurisdiction and multi-agency cooperation. In the US, public safety jurisdictions typically operate highly localized governance structures which can impede incident response effectiveness.[29] This organizational structure makes long-term planning difficult for standardization efforts and implementing interoperability of technology. Other factors which further complicate these efforts include the disparity of available funding and differences in public safety communications requirements for procurement and upgrade of radio equipment between jurisdictions and agencies. As a result, a complex web of separate LMR radio networks exists across the US utilizing different equipment from a variety of vendors across municipal, county, and state lines. Finding a solution to integrate these disparate LMR networks is essential to enhancing public safety and first responder capabilities during complex incidents.

Public safety communications networks are required to be secure, dependable, resilient, and accessible. Mobile broadband cellular networks currently deployed fall short of meeting public safety requirements and interoperability. PoC lacks cross-network interoperability. Over-the-top push-to-talk (OTT-PTT), which resides at the application layer, offers no mechanisms for network prioritization and lacks interoperability with PoC and other OTT-PTT applications. Although the planned public safety capabilities of mission critical LTE are expected to exceed those of legacy LMR and current PoC or OTT-PTT solutions, LMR will continue to exist as the primary public safety communications network for half-duplex PTT voice.

Interoperability of LMR and LTE MCPTT for PTT voice remains a significant problem for inter-agency and inter-municipal communications. Various standards and technologies exist to bridge LMR and LTE, but actual adoption remains low, and the need for inter-agency and inter-jurisdictions communications continues to grow. Until all jurisdictions and agencies migrate completely from LMR to a common MCPTT over LTE standard, a comprehensive solution to mitigate issues and provide interoperability for legacy LMR systems will be required.

The Inter-Working Function (IWF) is a mechanism for adapting LMR systems to mission critical systems using a common interoperability interface.[30] Specifically, an IWF for LMR and MCPTT allows LMR users on an LMR network to communicate with MCPTT users on an MCPTT network by adapting LMR protocol and data information to MCPTT systems flow. IWF Gateway procedures for group configuration, affiliation, management, regrouping, calls, broadcast, floor control, and security have been specified by 3GPP. Generally, an architecture for high level data flows has been defined, but the specific functionality and a particular deployment model has yet to be stated.

Four protocols, the Inter RF Subsystem Interface (ISSI), Console Subsystem Interface (CSSI), Digital Fixed Station Interface (DFSI) and Radio over IP (RoIP) have been identified as solutions to integrate separate Legacy P25 networks and wireless mobile broadband networks such as LTE through a common gateway interface:

---

[28] Chaudhry, A.U. and Hafez, R.H., 2019. LMR and LTE for Public Safety in 700 MHz Spectrum. Wireless Communications and Mobile Computing, Volume 2019, Article ID 7810546, 17 pages. https://doi.org/10.1155/2019/7810546

[29] Voss B and Anderson E. 2019. Interoperability of real-time public safety data: Challenges and possible future states. National Institute of Standards and Technology NIST.IR.8255.

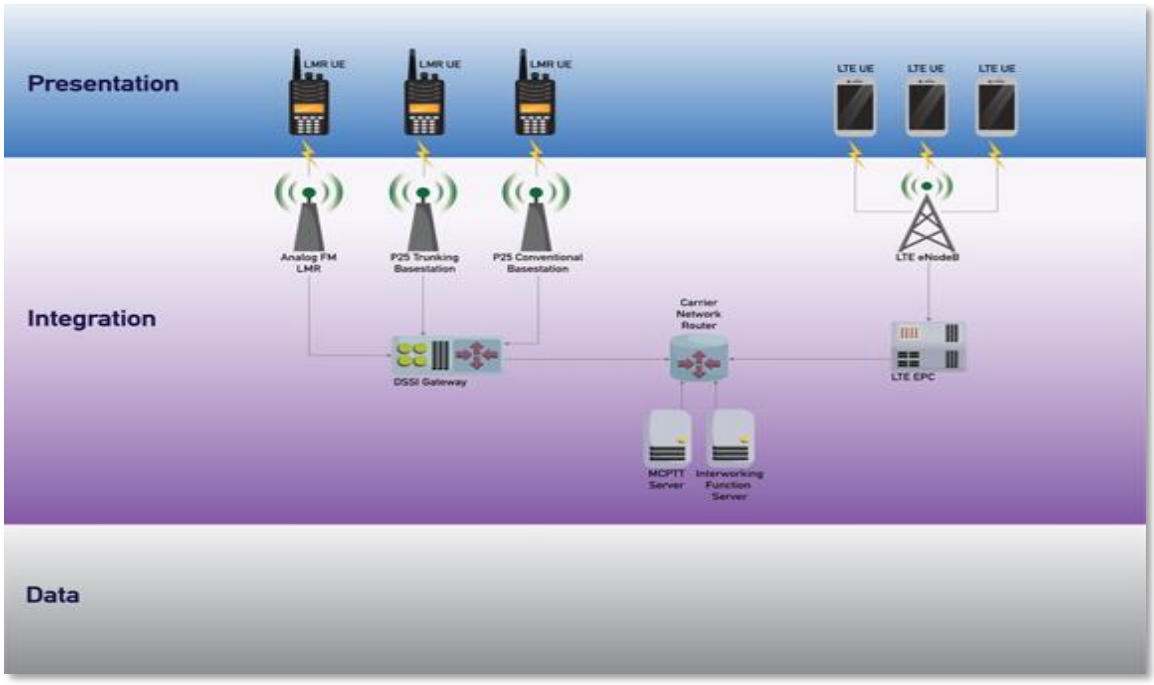
[30] European Telecommunications Standards Institute, 2018. Technical Report LTE; Mission Critical Communication Interworking with Land Mobile Radio Systems (3GPP TS 23.283 version 15.1.0 Release 15). European Telecommunications Standards Institute (ETSI) TS 123 283 V15.1.0 (2018-07)

- The ISSI could bridge legacy LMR and LTE networks as first responders eventually move towards mobile broadband technologies for mission critical voice, video, and data services. It is an IP-based connection designed to make P25 trunking systems interoperable and to support direct and group voice communications over different frequencies and carriers. Although, the P25 ISSI was initially made to interface between two P25 RFSSs, the ISSI can also be used to interface with an LTE device. Because of the flexibility in LTE design, the LTE core can mimic P25 RFSS abilities, and therefore, interface with LMR through ISSI. Unfortunately, ISSI is very expensive, making it a difficult solution for organizations with smaller budgets.

- CSSI is the console counterpart to ISSI. CSSI was designed to make console systems interoperable with P25 trunking systems. Along with ISSI, it is also technically rigorous, but very expensive.

- DFSI presents a simpler and more affordable alternative than ISSI to bridge legacy LMR and LTE networks. A solution for interoperability based on DFSI is illustrated in Apx Figure A-4. According to the Public Safety Technology Alliance's (PTSA's) LMR/LTE Interoperability Technical Subcommittee Report,[31] P25 DSFI with expanded functionality is suited to interconnect trunking and conventional P25 LMR and analog FM LMR network protocols. The DFSI is defined by TIA as an open-standard digital interface between a fixed station subsystem and a fixed station host which may be a P25 console subsystem or radio frequency subsystem [34]. A DFSI supports the P25 Common Air Interface and provides basic audio and control mechanisms between a fixed station and its host over full-duplex, half-duplex, and simplex communications. Specific advantages of P25 DFSI include the absence of intellectual property rights requirements for gateways, P25 encryption support, and the existence of formal conformance tests. Major drawbacks include the lack of floor control during voice communications, lack of support for certain audio vocoders, and lack of interoperability conformance tests. The PTSA views P25 DFSI as a near-term solution for legacy LMR and LMR-MCPTT Interoperability.

[31] Public Safety Technology Alliance, 2019. Land Mobile Radio (LMR)/Long Term Evolution (LTE) Interoperability Technical Subcommittee Report. Public Safety Technology Alliance (PSTA), Fremont, CA. Retrieved September 2019 from: https://www.pstalliance.org/technical-committees/subcommittee-report-and-comment-form/

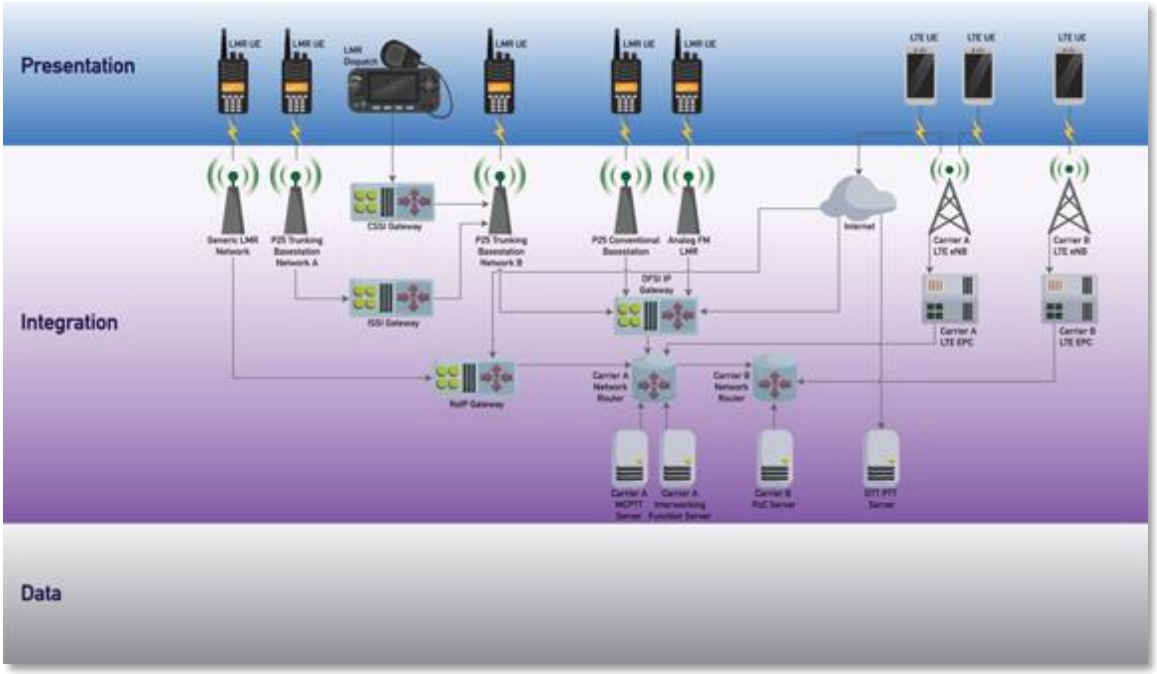


Apx Figure A-4: Generic View of an Interoperable System with LMR and MCPTT using DFSI.

Acronyms for Apx Figure A-4			
eNodeB	E-UTRAN Node B	MCPTT	Mission Critical Push-to-Talk
EPC	Evolved Packet Core	P25	Project 25
LMR	Land Mobile Radio	RoIP	Radio over Internet Protocol
LTE	Long-Term Evolution	UE	User Equipment

- RoIP addresses the drawbacks of P25 DFSI, making it a potential long-term solution to achieve interoperability between legacy LMR and MCPTT LTE functions. RoIP is a non-standard application of Voice of Internet Protocol (VoIP) technology to two-way radio communications. RoIP utilizes additional control functions for voice signaling and traffic control. Vendor specific and vendor-agnostic RoIP implementations are currently available on the market. RoIP does not support the transfer of device IDs between networks and requires a donor radio for connecting LMR and LTE networks. However, any LMR technology can be supported. According to the PTSA, standardization and expansion of current RoIP capabilities and functionalities should enable RoIP to become the preferred protocol for an LMR gateway.

A system overview of the possible solutions discussed above is depicted in Apx Figure A-5.



Apx Figure A-5: An Expanded View of an Interoperable System with LMR, MCPTT, OTT-PTT, and PoC using ISSI, CSSI, RoIP, and DFSI

Acronyms for Apx Figure A-5			
eNodeB	E-UTRAN Node B	MCPTT	Mission Critical Push-to-Talk
EPC	Evolved Packet Core	P25	Project 25
LMR	Land Mobile Radio	RoIP	Radio over Internet Protocol
LTE	Long-Term Evolution	UE	User Equipment

Once an interfacing protocol has been chosen, the system architecture of the interoperable network will need to be designed. One challenge to keep in mind is the difference in voice codecs used by P25 LMR and MCPTT. P25 LMR uses the voice codec AMBE while MCPTT uses the voice codec AMR. Therefore, to ensure interoperability, the IWF can facilitate LMR speech codec configuration in an MCPTT group. Another option is MCPTT to LMR communications can be transcoded by the IWF from AMBE to AMR. Transcoding is the process of digitally converting voice media formats to something readable for the target network. Further complications arise because each P25 network may use its own security and encryption protocols. Therefore, key sharing becomes costly and difficult. Instead of using many singular interfacial connections from each LMR network to the IWF, a central hub, connected to many LMR networks, hosting the particular interfacing protocol is a potential solution to alleviate management and implementation costs while increasing efficiency. The use of transcoding also requires re-encrypting the transcoded packets before it arrives at the end user's device to ensure end-to-end encryption. The network must also be secured for end-to-end security.

A potential high-level architecture that emphasizes modular and scalable design with a sophisticated encryption mechanism has been developed by the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) Next Generation First Responder (NGFR) Apex Program. This solution focuses on a central Responder SmartHub, where different, selected components, based on a particular first responder's needs and budget limitations, can be

connected using available open, as opposed to proprietary, standards and interfaces.[32] To ensure communications security, data in the system would be stored and sent with encryption to the Advanced Encryption Standard (AES) 256 level.[33] A Communications Module would host physical connections for voice communication devices, such as LMR and smart phones.

The Communications Module interfaces with the Controller Module, the main unit on the system that handles messaging and distribution of dispatch information. Therefore, the Communications Module integrates voice and data from LMR and LTE devices to be utilized by itself and the Controller Module. Together, the two modules would provide voice and data services, incorporating data priority, quality assurance, user system selection and control, and appropriate bandwidth allocation. Several other functions to be supported include specifications of network type, such as Bluetooth, 3G, LTE, FirstNet, Wi-Fi, radio voice and data, network status, network visibility, and network strength. A significant feature for voice communications is P25 compliancy. As mentioned previously in the LMR section, P25 compliancy ensures compatibility with existing legacy and LMR systems.[34] Furthermore, NGFR systems would be able to send and receive real-time audio and video amongst each other. Data would be shareable among all systems that adhere to NGFR data standards, protocols and connectivity guidelines. Responders would be able to transmit and receive voice, data, and video to and from current communications infrastructure as well as future NGFR systems.

An interoperable system is paramount to ensuring the safety of public safety officers and the general public. Research is still being conducted to find and deploy the optimal solution. One such area is the interconnection from NG911 systems and the broadband service provider as technical specifications for this connection have yet to be established. An example of recent efforts in this area can be found in the 911.gov report "*The Critical Need for Communications,*" which speaks to the importance of understanding the two-way exchange of data and information between NG911 systems and users of public safety broadband networks.

A.5.5 National Public Safety Broadband Network (NPSBN)

The First Responder Network Authority (FirstNet Authority), along with AT&T, has been tasked with managing the establishment, operation, and maintenance of the National Public Safety Broadband Network (NPSBN) [25]. As of early 2018, all fifty-six states and territories have opted in and granted AT&T permission to deploy the network in their corresponding state or territory. However, adoption of the network is still up to each individual public safety agency. NPSBN has been designed to incorporate attractive capabilities that are required and important for the public safety organization. Necessary capabilities are voice and data, with the appropriate priority and preemption services, interoperability, GIS, and integration of applications.

NPSBN uses a combination of Voice over Long-Term Evolution (VoLTE) and push to talk over cellular (PoC) for voice communications. VoLTE is a Voice over Internet Protocol (VoIP) adaptation that delivers high-speed wireless one-to-one voice communications. PoC is a form of critical one-to-one and one-to-many voice correspondence. VoLTE and PoC also offer data transmission over cellular. While VoLTE separates its voice and data streams, PoC aggregates the two data types into one channel.

VoLTE's separation scheme allows it to give high priority and guaranteed allocated resources to its voice channel while downsizing the priority and resources for its data stream. Voice over PoC suffers from lower priority and non-guaranteed resources along with its data. Because voice is the primary form of communications for first responders, PoC is not the recommended form for mission-critical talk. Instead, MCPTT (Mission Critical Push-to-Talk), the 3GPP standardization

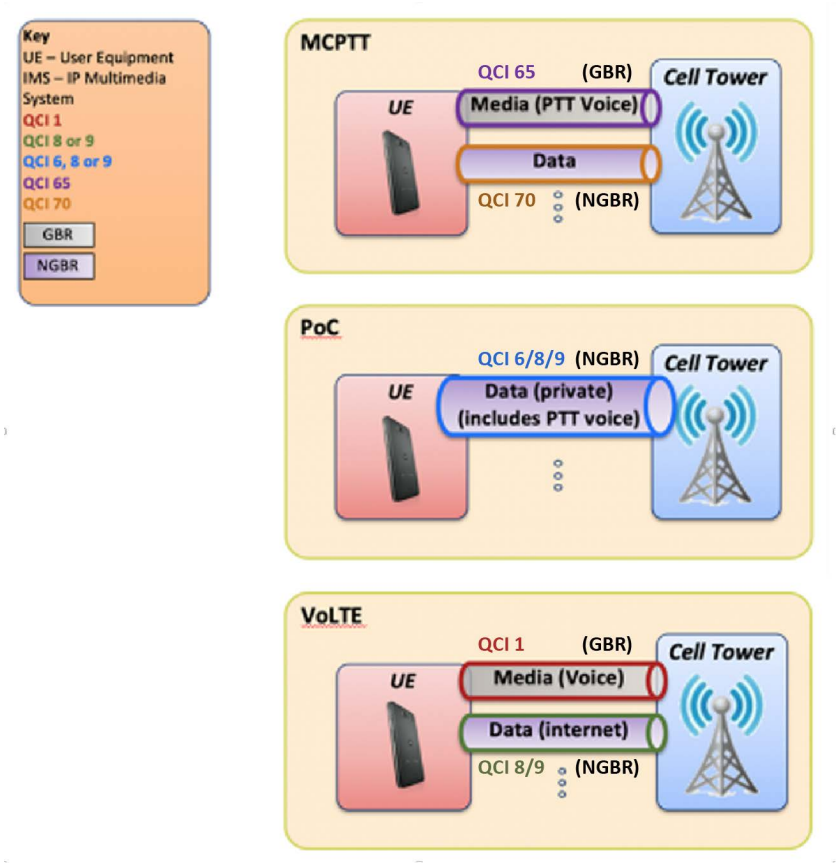
---

[32] DHS, 2018. Next Generation First Responder (NGFR) Integration Handbook Version 3.0 - Part 1: Introduction. August 2018. US Department of Homeland Security Science and Technology.

[33] DHS, 2018. Next Generation First Responder (NGFR) Integration Handbook Version 3.0 - Part 2: Engineering Design. August 2018. US Department of Homeland Security Science and Technology.

[34] DHS, 2018. Next Generation First Responder (NGFR) Integration Handbook Version 3.0 - Part 3: Technical Supplement. August 2018. US Department of Homeland Security Science and Technology.

for mission-critical communications, is the optimal solution. Similar to VoLTE, MCPTT separates its voice and data channels, has higher priority than VoLTE, and has allocated resources. However, the NPSBN has yet to integrate MCPTT into its devices. Apx Figure A-6 compares the different data streams among VoLTE, PoC, and MCPTT.



Apx Figure A-6: Comparison of MCPTT, PoC, and VoLTE Transmission of Voice and Data

As a comparison metric, Apx Figure A-6 includes information about the QCIs of each of the standards. QCIs control the prioritization and scheduling of data throughout the network. A QCI is an integer parameter that holds QoS (Quality of Service) information, such as priority, resource type, allowed packet delay, and allowed packet error loss rate.[35] Apx Table A-1 lists the different QCI values and their characteristics.

Apx Table A-1: Standard LTE QCI Table [39]

QCI	Resource Type	Priority	Delay Budget (ms)	Packet Loss Rate	Example Service
1	GBR	2	100	10^{-2}	Conversational Voice (VoLTE)
2		4	150	10^{-3}	Conversational Video (video chat)
3		3	50		Real-time gaming

[35] European Telecommunications Standards Institute, 2014. Digital Cellular Telecommunications System (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Policy and Charging Control Architecture (3GPP TS 23.203 Version 12.6.0 Release 12). European Telecommunications Standards Institute (ETSI) TS 123 203 V12.6.0 (2014-09)

4		5	300	10^{-6}	Non-Conversational Video (buffered streaming)
65		0.7	75	10^{-2}	Mission Critical PTT Voice
66		2	100	10^{-2}	Non-Mission Critical PTT Voice
5	NGBR	1	100	10^{-6}	IMS Signaling
6		6	300		Video (Buffered Streaming), TCP-based services
7		7	100	10^{-3}	Video (live streaming), Interactive Gaming
8		8	300	10^{-6}	TCP-bases services (e.g. web browsing, email, FTP)
9		9			
69		0.5	60	10^{-6}	Mission Critical Delay Sensitive Signaling
70		5.5	200	10^{-6}	Mission Critical Data

Also shown in Apx Table A-1, NPSBN compatible devices support enhanced priority services, and thus, are given a different QCI from a commercial user. Due to proprietary reasons, the network scheduling algorithm is not publicly available. However, if one assumes a round robin scheduler, which is a commonly used algorithm where each transmission job is given the same time to transmit before that job is paused and another a job is begun, an NPSBN data transmission would be allowed to send more resource blocks during each transmission because of its QCI. Therefore, a first responder would be able to send a considerable amount more data than a public user in the same time span.

Apx Table A-2 compares Access Class (AC), Establishment Cause, and Allocation and Retention Priority (ARP) values. ACs determine when, if at all, the User Equipment (UE) can access the LTE radio interface based on situations defined by Radio Resource Control (RRC) establishment causes. An RRC establishment cause indicates the reason for the connection request between the UE and the eNB (Evolved Node B), the LTE base station in the Radio Access Network (RAN) .

Establishment causes include emergency, Mobile Originating (MO) signaling, MO data, and Mobile Terminating (MT) access. Allocation and Retention Priority (ARP) designates the bearers' priority levels for allocation and retention. UEs with access classes 10 to 15 are automatically given the High Priority Access (HPA) establishment cause. Devices operating on the NPSBN have AC 11 while public users have values ranging from 0 to 9. Consequently, during times of congestion, eNB prioritizes NPSBN requests, and public user requests will be prevented from consuming limited radio resources. Furthermore, consumer users with AC 0 to 9 are subject to Access Class Barring (ACB), which dictates if and when a user can access a particular eNB. This restricts the load on a particular base station. UEs with AC 11 to 15 have a different ACB parameter, which is a Boolean indicating whether or not it is eligible for ACB [40]. NPSBN UEs in particular are exempt from ACB, and as a result, they do not have to wait for tower connectivity. Thus, a higher precedent access class and establishment cause give NPSBN user's specialized treatment to the radio air interface.

In Apx Table A-2, Commercial Solutions for Classified (CSfC) is the use of commercial products for the protection of classified data. NS/EP (National Security/Emergency Preparedness) has been included for comparison. Note in Apx Table A-2 that NPSBN also has a better Access Class (AC) than regular commercial users.

Apx Table A-2: Common Parameters for Access Priority

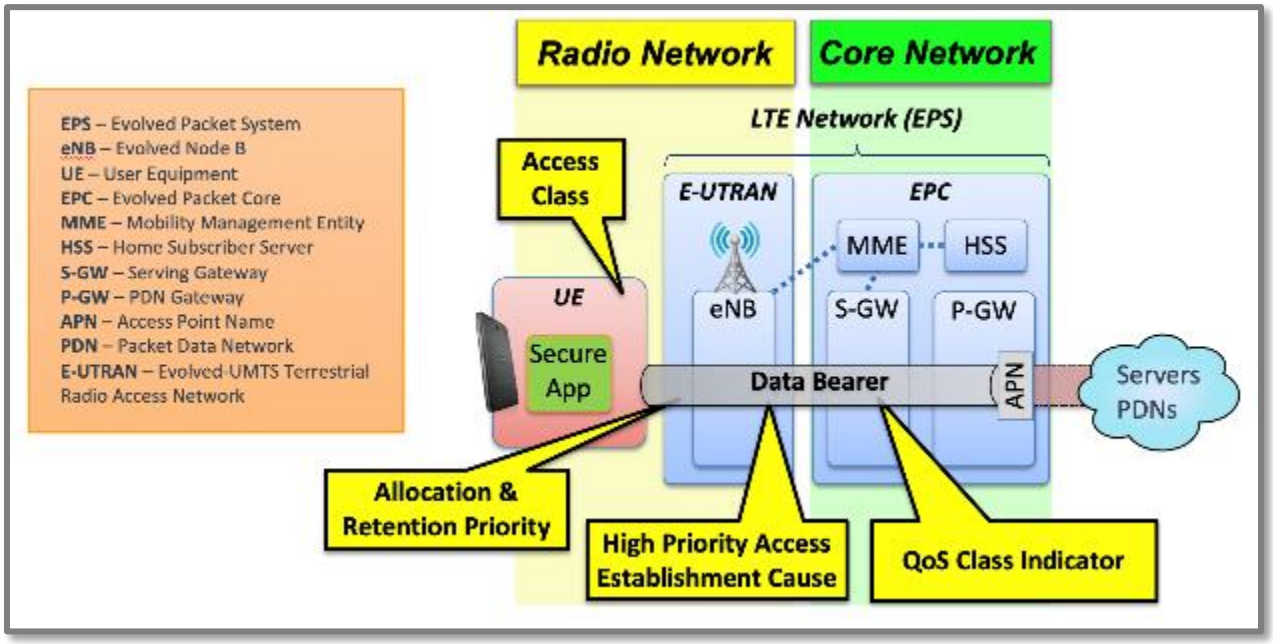
Attribute	NS/EP Value	NPSBN Value	Public User Value
Access Class	14	12	0 to 9
Establishment Cause	High Priority Access	High Priority Access	MO signaling or Emergency
ARP	1 – 3	4 – 6	7 – 15

The access class and RCC establishment cause additionally determine the bearer used. Bearers are the gateways that connect the device to packet data networks (PDNs), the networks that deliver data services. The Internet is an example of a PDN. Depending on the bearer's QCI value (see Apx Figure A-6), the bearer can either be Guaranteed Bit Rate (GBR)

or Non-Guaranteed Bit Rate (NGBR).[36] GBR bearers are pre-allocated and ready to deliver data at a guaranteed rate. NGBR bearers are not allocated but instead transfer data on a best-effort basis.[37]

Furthermore, NGBR is vulnerable to packet losses while GBR is not. Another important attribute regarding bearers is Allocation and Retention Priority (ARP), which designates the bearers' priority levels for allocation and retention. In particular, during times of network congestion and resource limitation, ARP determines whether an EPS bearer establishment or modification request would be accepted or rejected. A lower numeric value corresponds to a higher priority ARP. Apx Table A-2 demonstrates NPSBN transmissions have values 4 to 6, while public users have 7 to 15. NPSBN transmissions have higher priority, and therefore, have a greater likelihood of receiving the necessary network resources during times of high traffic.

The consolidation of better access class, establishment causes, and ARP, represented in Apx Table A-2, allows for fast and high quality data streaming for NPSBN users.



Apx Figure A-7: LTE Network Architecture

In Apx Figure A-7, the E-UTRAN controls the radio communications with the UE, while the EPC contains multiple components that facilitate the proper transfer of data between the eNB and the external PDNs. The specific PDN requested is dependent upon the Access Point Name (APN). Further details are available in Advanced Communications Video over LTE: Efficient Network Utilization Research.[38]

---

[36] Ekstrom H, 2009. QoS Control in the 3GPP Evolved Packet System, IEEE Communication Magazine, 47(2):76-83, February 2009.

[37] Kassa B, 2018. Quality of Service Priority and Preemption. National Public Safety Telecommunications Council (NPSTC) FirstNet. Retrieved September 2019 from: http://www.npstc.org/download.jsp?tableId=37&column=217&id=3685&file=FirstNet_QPP_Intro.pdf.

[38] JHU APL, 2015. Advanced communications video over LTE: efficient network utilization research, JHU APL Report AOS-15-1005 to the US Department of Homeland Security Science and Technology.

Public safety users are able to preempt secondary users on NPSBN. Because the FirstNet Authority has entered a Covered Leasing Agreement (CLA) with AT&T, AT&T is permitted to utilize the NPSBN spectrum for secondary commercial cellular service. However, when incident situations necessitate public safety-only spectrum usage, first responders will be prioritized over other commercial users. NPSBN's addition of preemption is yet another desirable feature for the public safety sector.[39]

Although the features QCI, AC, establishment cause, ARP, and preemption are useful, they are not all-encompassing. As stated before, these features combine to enhance the priority services for NPSBN users, but they still fall short of MCPTT. MCPTT offers better priority services as shown in Apx Table A-1 and Apx Table A-2. One way to make NPSBN closer in standards to MCPTT is through the addition of Wireless Priority Services (WPS). WPS is a federal program that authorizes cellular communications service providers to prioritize urgent calls and avoid congestion through wireless networks.[40] NPSBN users can use WPS to upgrade their voice priority services. It is important to note that WPS does not increase data priorities.

In addition, NPSBN lacks another key feature included in MCPTT. Off-network, direct device-to-device (D-D) communications is included in MCPTT. PoC currently does not have this capability. D-D communications are extremely important for first responders because D-D provides reliable communications in remote locations without network support or during times of network failure. The 3GPP Release 15 Vehicle to Everything (V2X) communications technology[41] may provide off-network D-D capabilities but, until then, LMR voice communications is still required for off-network D-D communications.

Standardization of PoC through the Open Mobile Alliance (OMA) has paved the way to introduce interoperability between NPSBN and other networks. Networks that employ the standards-based OMA PoC system can connect with one another through the PoC Network-to-Network (NNI) interface. This will enable cross-carrier communication. Furthermore, interoperability between OMA PoC with P25 LMR systems can be done through interworking functions.[42] Detailed discussion of LTE-LMR interoperability can be found in the Interoperability Issues and Proposed Solutions Section 6.4 of this report. One vendor has also provided a strategy for interoperability with NPSBN and non-NPSBN users. Their solution is a part of their Media Cohesion Framework (MCF) implementation, and the framework as a whole has been successfully tested and installed among several NPSBN trial systems. The interoperable solution in MCF includes utilization of an infrastructure bridge. This requires the ability of all collaborating networks (NPSBN, commercial, LMR, etc.) to be able to reach a common data center that hosts network interconnection services. Technology bridges are inserted between the network and the data center to ensure data format compatibility. To augment the infrastructure bridge, an ad-hoc on-scene system can be employed. This method enables dynamic communication between responding units and ensures capabilities when certain resources from the wide-area infrastructure are absent.[43] Thus,

---

[39] Kassa B, 2018. Quality of Service Priority and Preemption. National Public Safety Telecommunications Council (NPSTC) FirstNet. Retrieved September 2019 from: http://www.npstc.org/download.jsp?tableId=37&column=217&id=3685&file=FirstNet_QPP_Intro.pdf.

[40] Federal Communications Commission, 2014. Wireless Priority Service (WPS). Federal Communications Commission, 21 May 2014. Retrieved September 2019 from: https://www.fcc.gov/general/wireless-priority-service-wps

[41] European Telecommunications Standards Institute, 2018. Technical Report LTE; Service requirements for V2X services (3GPP TS 22.185 version 15.0.0 Release 15). European Telecommunications Standards Institute (ETSI) TS 122 185 V15.0.0 (2018-07)

[42] Kodiak Networks Inc., 2012. Response to NTIA Notice of Inquiry On Requirements On Behalf of the First Responder Network Authority. National Telecommunications and Information Administration (NTIA), US Department of Commerce. Retrieved September 2019 from: https://www.ntia.doc.gov/files/ntia/kodiak_networks_response.pdf

[43] Mutualink Inc., 2014. Embracing FirstNet Collaboration Opportunities. Mutualink Version 1.1. Retrieved September 2019 from: https://mutualink.net/wp-content/uploads/2016/05/FirstNet-Collaboration-12-3-14.pdf

plans for cross-network and cross-carrier communication between users on NPSBN and users on other networks have been established and deployed.

GIS is a framework designed to gather, store, analyze, and present spatial data. Along with the location of other personnel and resources, GIS map and structure layers can also provide vital situational awareness at emergency sites. GIS helps emergency responders navigate incident sites effectively and efficiently. NPSBN has acquired GIS layers, or geographic data, from states to augment its system. Information such as ferry terminals, bus and rail terminals, heliports, tribal areas, and rural health primary care areas has been collected and integrated into NPSBN.[44]

Third party applications are managed through the NPSBN App Catalog. The NPSBN App store filters the applications through two categories: certified and listed. A summary of requirements between these two categories is depicted in Apx Table A-3.

Apx Table A-3: FirstNet application requirements for certified and listed apps

Assessment	Certified	Listed	Description
Relevancy	Yes	Yes	NPSBN apps should be designed to support public safety.
Availability	Yes	Yes	NPSBN apps, along with their associated middleware and backends, should have high availability and minimal downtime.
Scalability	Yes	No	NPSBN apps should be able to scale to the demand of public safety without incurring issues. For example, apps should be able to handle load spikes that may occur in emergency situations.
Resiliency	Yes	No	NPSBN apps should be able to handle exceptions gracefully with minimal effect on the user experience.
Data Privacy	Yes	Yes	NPSBN apps that collect data must be able to keep data secure and private.
Resource Usage	Yes	No	NPSBN apps should be optimized to have minimal usage impact, in terms of battery and data usage, storage, etc., on the user's device.
Security	Yes	Yes	NPSBN apps must ensure that proper security steps, such as data encryption and penetration testing, have been taken in all aspects of the app.

Certified apps have gone through a rigorous assessment to prove scalability, resiliency, and resource usage along with approvals, such as relevancy, availability, data privacy, and security; listed apps must do this as well. Scalability allows flexibility to the demands of the public safety system. Resilient apps handle exceptions gracefully with minimal effect on the user experience. Battery usage, storage capacity, and other user device features must be minimally impacted. Therefore, NPSBN apps should be optimal and efficient. Both certified and listed apps must be designed to support public safety, keep data and devices secure, be highly available, and hold minimal downtime.[45] The process implemented to ensure the categorization of certified and listed apps not only ensures a robust system but also preemptively prepares for future interoperability. Generally, NPSBN has a thorough application quality control process, which guarantees an enhanced and secure communication experience for first responders.

In conclusion, NPSBN is an LTE broadband network with data capabilities to significantly enhance the current public safety communications infrastructure. However, new technology and further updates, such as the addition of MCPTT,

[44] Kennedy TJ, 2017. FirstNet an Overview of Program and Techniques Used for Public Safety Data Collection. National Security and Public Safety Summit, 8 July 2017, Environmental Systems Research Institute, Redlands, CA. Plenary Presentation. Retrieved September 2019 from: http://proceedings.esri.com/library/userconf/nss17/papers/nss_06.pdf

[45] https://developer.firstnet.com/firstnet/resources/development#title-description-1

must be accomplished before its voice capability can readily replace existing LMR systems. Overall, NPSBN is a significant step in addressing the need for public safety communications robustness and interoperability.

A.6 Identity, Credential, and Access Management Implications

While interoperability relies on the ability to access data hosted across multiple agencies, access to data must be securely controlled to prevent unauthorized access. Data providers often have their own authentication services resulting in users requiring unique credentials for accessing different systems or networks. Allowing discovery and access to data from multiple data providers requires the integration layer to use a standardized approach to authentication so participating entities can validate and trust the identities of users attempting to log in to their systems. Using trusted, interoperable authentication services will minimize the number of required credentials and achieve efficiencies by eliminating stand-alone authentication services.

Not every user should have or needs to have access to all data sources. After identities are authenticated, the users' unique attributes determine if access to specific information is authorized. These user attributes require dynamic management to inform access decisions, including provisions for agile updates and removal of user access. Both policy and technical alignment across departments and agencies will enable implementation of interoperable capabilities so that there is a trusted confirmation of appropriate users and their access to mission-relevant information.[46]

Identity, Credential, and Access Management (ICAM) refers to the policies and technical tools that allow an organization to manage, monitor, and provide secure access to their protected data.[47] ICAM enables authorized individuals or agents to have appropriately calibrated and independently verifiable access to information enterprise, comprising physical facilities, devices, systems, networks, applications, virtual digital libraries, and digital information shares. Those authorized would then be able to conduct research, initiate a query, discover information they seek, and request, receive, process, and post information.

In order to tackle this problem at the federal enterprise level, the Federal ICAM (FICAM) roadmap effort was established in 2009 and version 2.0 of the FICAM roadmap was published in 2011.[48] The FICAM program is managed by the General Services Administration's Office of Information Integrity and Access and is meant to provide a common set of ICAM standards, best practices, and implementation guidance. The FICAM architecture (Apx Figure A-8) is a conceptual blueprint for designing, planning, and implementing ICAM.[49]

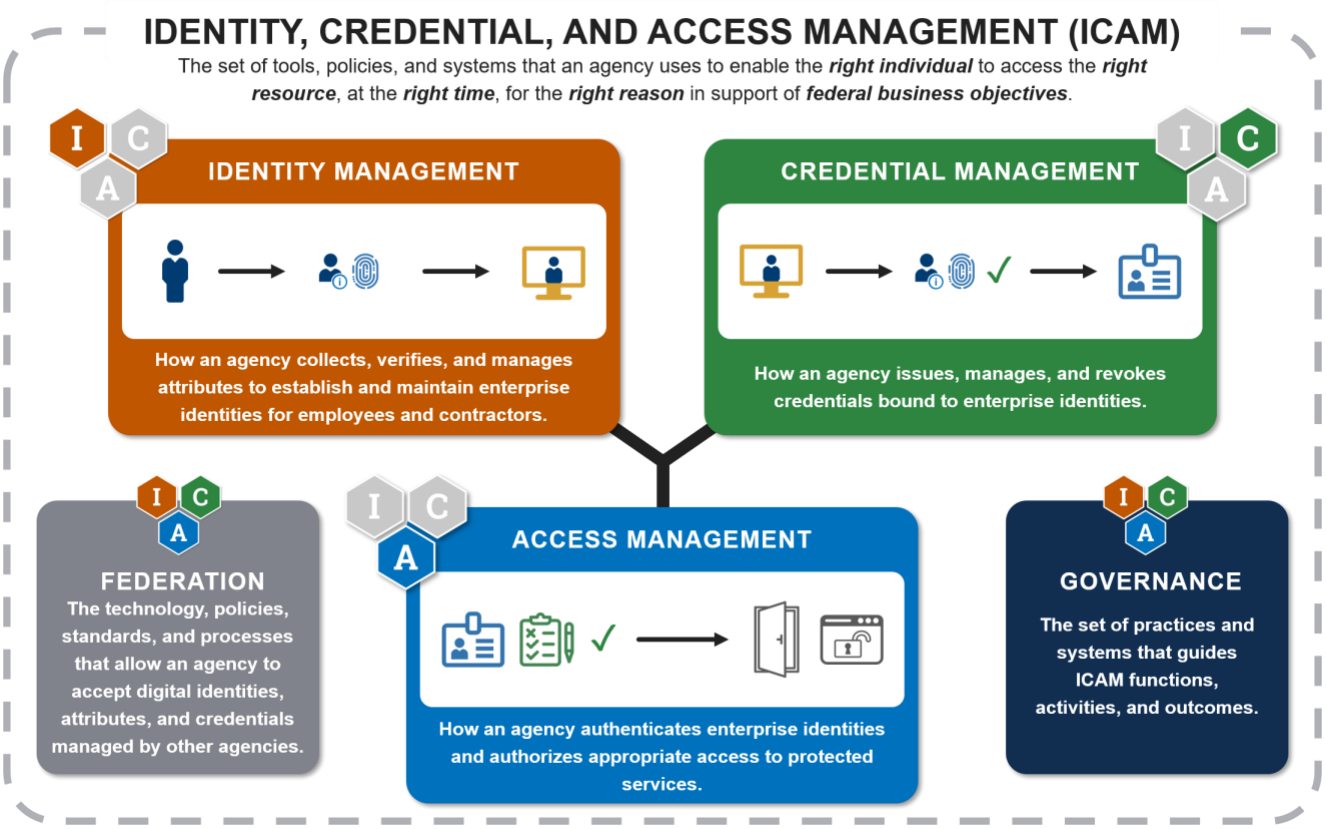
---

[46] The White House, 2012. National Strategy for Information Sharing and Safeguarding. US Government Printing Office. December 2012.

[47] National Public Safety Telecommunications Council (NPSTC) Mission Critical Push to Talk Considerations for the Management of User ID and First Responder Identity. Final Report, 8 January 2018.

[48] Federal Chief Information Officers Council, 2011. Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, Version 2.0. US Government Printing Office. 2 December 2011.

[49] Federal Chief Information Officers, 2019. Federal Identity, Credential, and Access Management Architecture. Retrieved October 2019 from https://arch.idmanagement.gov/



Apx Figure A-8: View of ICAM [24]

In general usage, ICAM consists of the following:

1. **Identity**: The process by which a unique representation of a user is established. Examples include Name, Address, Date of Birth, Social Security Number, Place of Birth, Birth Certificate, Driver's License, and other government issued identification, including passport or naturalization certificate or resident-alien card. Identity is further enriched by physical information (height, weight, color of hair, color of eyes) or bio-metrics such as retina or fingerprint.
2. **Credentials**: The process by which physical, digital, or other tokens (what you have), and additionally, memorized phrases (what you know) are established to enable authentication of users whose identity was previously established. Examples include Department of Defense Common Access Card (DoD CAC), Department of Homeland Security Personal Identity Verification (DHS PIV), Driver's License, user-id + password, public-key certificates, digital tokens (such as HID or RSA), code words, etc. These serve to establish that a user is authorized based on independently established identity.
3. **Authentication**: The process by which an entity (network, device, application, system, etc.) verifies the identity using credentials appropriate for that circumstance. This may be done using multi-factor authentication or single-factor authentication. Examples include: Login/password; Login/password + answer to a preregistered question; PIN + CAC/PIV; Login + Password + Code + HID/RSA Token generated code; PIN with digital certificates; or specially generated web URL or code sent to a device, along with a single-factor authentication.
4. **Access**: The process by which an authenticated user is given access to a network, device, system, application, information store, etc. User's membership, roles, and responsibilities are captured as privileges accorded to the user so that the user is able to gain access to a medium (network, device, system, etc.) and then is able to view, research, explore, select, download, process, upload, or modify/delete information.

5. **Management**: The policies and processes for information relating to users' identities and corresponding strength of the identification; their assigned credentials and the currency (active/expired/one-time/persistent, expiration date, renewals); the issuing agency and strength of authentication based on single-factor or multi-factor methods; and establishing and maintaining information about memberships, roles, and responsibilities, and associating them to individual or groups of users to support access mechanisms. There are overall management processes and polices for covering ICAM and more specific ones for each of the topical areas:

    a. Identity
    b. Credentials
    c. Authentication
    d. Access

As an emergency first responder architecture, the ISF should address the following:

- ICAM Governance is needed to guide, enable, and manage coordination, collaboration, and access for first responders across all use cases. A governance body establishes overall policies for ICAM, enforces these policies, and independently validates compliance to these policies to ensure that information integrity is maintained while authorized users are assured access and ability to modify information as and when they need.
- Federated identity management is needed to ensure credentials, authentication, and access are based on strong and verifiable underlying identities. Federated identity management links a user's identity across multiple security domains, each of which may have its own identity management, and is an agreement among multiple agencies or resources to allow access by users via the same identification data.
- An adaptive flexible approach is necessary for credentials in recognition of the difficult and varied operational situations for first-responders. Adaptive management of access should be based on types of emergency situations, strength of credentials, and authentication. For example, access to resources may be more open initially when support is sparse and the situation is dire. But, as the situation improves and better support and infrastructure arrives over time, access may need to revert to more rigorous enforcement of policies appropriate for the use-case.

A.7 Future Public Safety Answering Point/ Next Generation 911

Staff at Emergency Communications Centers (ECCs) answer calls for emergency services and dispatch police, firefighting, and ambulance services to incidents as required. Most of the information used to support public safety comes from the public and much of that information is collected at ECCs. Initial notification of many, if not most, incidents begins when an emergency (911) call is received at an ECC. The ability of staff to obtain as much relevant data from callers, to respond appropriately to the provided information, and to identify, locate, and dispatch the appropriate services is critical to achieving the public safety mission. In addition, ECC operators need to be able to communicate accurate information, based upon interviews with callers, to first responders prior to their arrival at an incident scene.

To aid call center operators, ECCs are equipped with CAD, GIS Mapping, and Record Management Systems (RMS). These systems enable ECC operators to locate needed resources, dispatch available first responders, and provide them any additional information required to complete their mission. ECC operators also have access to metadata from 911 calls to enable them to identify and locate callers. CAD Systems are a key conduit for data passing through ECCs to first responders.

The existing ECC infrastructure has served the nation well for decades; however, as a result of the recent, rapid evolution of telecommunications technologies, that infrastructure now faces obsolescence. Designed to support the passing of analog calls over circuit-switching networks, existing call center technology has not kept pace with changes in the overarching telecommunications infrastructure. Beginning in the 1960's, the Public Switched Telephone Network (PSTN), sometimes referred to as the Plain Old Telephone Service (POTS), which is the basis for landline service, began the transition from analog to digital technology. Land Mobile Radio made a similar transition to digital transmission, and with the adoption of the P25 standard, most of the nation's LMR infrastructure is now also digital. In the 1990's,

packet-switching technologies emerged enabling the Internet to become an effective, efficient and, within approximately a decade, ubiquitous form of electronic data communications. Between 1997 and 2009, home Internet access more than tripled from 18% of US households in 1997 to 68.7% in 2009.[49] At approximately the same time, cellular telephone service emerged by combining both traditional circuit switching for voice and Internet Protocol (IP) based packet switching for data. Between 1998 and 2005, the number of US household with a cell phone doubled from 36% to 71%.[50] Today, 96% of adults own a cell phone and 81% own a smart phone, which combines access to a mobile telephone network and robust Internet connectivity.[50]

This evolution in telecommunications presents two problems for the 911 system. First, the proliferation of smart phones has greatly increased call volume. As recently as thirty years ago, a significant incident might have sent a couple of observers searching for a nearby landline in order to alert a call center. Today, a half dozen or even a dozen observers could conceivably be on their smart phones within minutes. During Hurricane Harvey and other recent storms, call centers have been overwhelmed so that many calls went unanswered. Callers with urgent needs often had to wait for service and assistance.[51]

The second problem is that the analog technology on which most call centers are based does not support many of the features provided by IP based technology. In particular, most existing ECCs are not equipped to receive text or multimedia data from the public. ECC technology is out of step with the ways in which people communicate today.

Next Generation 911 will enhance the capability and reliability of 911 services to create a faster, more resilient system that allows the public to provide voice, photos, videos, and text messages seamlessly to the 911 network. It will also improve the ability of ECCs to manage call overload, natural disasters, and the assignment of 911 calls and responses based on location tracking.[52]

Next Generation 911 will provide first responders a secure system based upon Internet Protocol (IP)-based technology and open standards. There are approximately 6000 ECCs in operation across the nation, operating in a silo environment.[53] In addition to modernizing technology to adopt IP standards, Next Generation 911 hopes to improve interconnectivity between ECCs. Features of the upgraded ECCs will include:

- The ability to process all types of emergency calls, including voice, text, data, and multimedia information: Implementation of IP-based technology will enable ECCs to receive, process, and disseminate images and video. This implementation has the potential to enhance decision making as incident commanders, on-scene and remote, will be able to better visualize the incidents to which they are responding. Increased use of text messaging may mitigate concerns about high throughput at call centers. Text messaging places less demand on communications networks and on call center workers, who can scan text messages and identify the most urgent far more rapidly than they can voice calls.
- Integration of CAD systems: Adoption of open standards has the potential to enhance data exchange between CAD systems and external data sources, especially public sources. One can readily envision a capability to receive relevant data from the public at the scene of an incident, input that data into the CAD system, and

[50]Pew Research Center, 2019. Mobile Fact Sheet. Pew Research Center Internet and Technology. The Pew Charitable Trusts. Retrieved September 2019 from: https://www.pewinternet.org/fact-sheet/mobile/

[51]CBS News, 2017. Houston emergency officials tell 911 callers not to hang up. CBS News 29 August 2017. Retrieved September 2019 from: https://www.cbsnews.com/news/houston-flooding-911-calls-after-harvey/

[52]National Highway Traffic Safety Administration, 2019. Next Generation 911. National 911 Program, Office of Emergency Medical Services, National Highway Traffic Safety Administration. Retrieved September 2019 from: https://www.911.gov/issue_nextgeneration911.html

[53]National Highway Traffic Safety Administration, 2019. NG911 Roadmap: pathways toward nationwide interconnection of 911 services. Version 1.0. Retrieved September 2019 from: https://www.911.gov/pdf/NG911_Roadmap_Final.pdf

disseminate that data to incident commanders on scene. Ideally, this would lead to first responders being able to interact with and accept data from CAD systems while operating in jurisdictions outside their own.

- Enhanced routing of 911 calls to call centers based upon location and capacity: Next Generation 911 centers will have the ability to route calls to ECCs with the jurisdiction and capacity to service the calls. In times of heightened demand, this capability could be used to balance loading across ECCs.
- Improved interoperability between call centers: Thirteen states have deployed statewide Emergency Service Internet Protocol Networks (ESINets) connecting emergency response resources. It is envisioned that, as a result of Next Generation 911, ECCs across the nation would be connected as part of a nationwide broadband ESINet.[54] A potential advantage of improved interoperability between ECCs is the emergence of a national 911 database as emergency data is shared on a nationwide basis.
- Nationwide Identity, Credential, and Access Management capability: First responders should be able to log on once to the system and have access to the full range of datasets for which they are authorized without additional action.
- Access to data from non-traditional entities: Non-traditional entities can range from suicide hotlines to social media networks.
- Access to GIS data and applications: Real-time GIS resources can greatly enhance first responder situational awareness and enable the ability to locate a caller with their coordinates on a map. A goal of Next Generation 911 is to make real-time GIS resources broadly available across the public safety community.

Implementation of a NG911 capability involves more than new computer hardware and software. It will require coordination among emergency communications, public safety, and legislative and governing bodies.[54] Achieving these objectives will require overcoming a number of technological and other hurdles, most notably, the development and promulgation of the following:

- Open standards to support interoperability between ESInets
- Nationwide cybersecurity standards
- Carrier migration and delivery standards
- Testing regimens
- Data standards, including a common data model

In addition, achieving the envisioned NG911 capabilities will also involve dealing with a number of operational issues.

- Cross-jurisdictional call handling
- Expanded workloads at ECCs – this includes sorting dozens of images and/or videos from the public and determining which to transmit to responders

Over time, as communications and other relevant technologies evolve, there will be a need for NG911 capabilities to evolve to better handle the needs of all the agencies involved.

[54]National Highway Traffic Safety Administration, 2018. Next Generation 911 Cost Estimate: A Report to Congress. October 2018. National 911 Program, Office of Emergency Medical Services, National Highway Traffic Safety Administration and National Telecommunications and Information Administration.

A.8 Additional Resources Bibliography

- 3GPP, 2019. Keywords and Acronyms. Retrieved October 2019 from https://www.3gpp.org/technologies/keywords-acronyms/
- Contestabile J. (2011). Concepts on information sharing and interoperability. Domestic Preparedness, 23 March 2011. Accessed 15 February 2018 and available at: https://domesticpreparedness.com/preparedness/concepts-on-information-sharing-and-interoperability/
- Commins J, 2019. Six Keys to Hospital Interoperability. Health Leaders, 22 January 2019. Retrieved October 2019 from https://www.healthleadersmedia.com/6-keys-hospital-interoperability
- Department of Defense Considerations for Disaster Response State of the Art Report, Homeland Defense and Security Information Analysis Center (HDIAC), 2018.
- DHS SAFECOM, 2018. Emergency Communications Governance Guide for State, Local, Tribal, and Territorial Officials. Department of Homeland Security SAFECOM. Retrieved October 2019 from: https://www.dhs.gov/publication/governance-documents
- Fimin F, 2019. The Evolved Packet Core. 3GPP: the Mobile Broadband Standard. Retrieved October 2019 from https://www.3gpp.org/technologies/keywords-acronyms/100-the-evolved-packet-core
- LTE Encyclopedia, 2019. LTE Network Infrastructure and Elements. Retrieved October 2019 from https://sites.google.com/site/lteencyclopedia/lte-network-infrastructure-and-elements
- Mitchell B, 2019. What is Cloud Computing? Lifewire Publishing, 16 May 2019. Retrieved September 2019 from: https://www.lifewire.com/what-is-cloud-computing-817770
- National Institute of Standards and Technology (NIST) Information Technology Library Computer Resource Center (CSRC)
- National Institute of Standards and Technology (NIST), 2018. Big Data Interoperability Framework: Volume 1, Definitions. NIST Special Publication 1500-1r1. NIST Big Data Public Working Group Definitions and Taxonomies Subgroup, Version 2, June 2018.
- National Public Safety Telecommunications Council (NPSTC), 2019. Public Safety Internet of Things Use Cases covering Multiple Disciplines. Draft March 2019. NPSTC Technology and Broadband Committee, Public Safety Internet of Things Working Group, NPSTC.
- Open Connectivity Foundation, 2019. Solving the IoT Standards Gap. Retrieved October 2019 from https://openconnectivity.org/
- National Highway Traffic Safety Administration, 2016. Next Generation 911 Procurement Guidance. National 911 Program, Office of Emergency Medical Services, National Highway Traffic Safety Administration and National Telecommunications and Information Administration. Retrieved October 2019 from: https://www.911.gov/project_nextgeneration911procurementguidance.html and https://www.911.gov/pdf/National_911_Program_NG911_Procurement_Guidance_2016.pdf
- Computer Security Resource Center, 2019. Mobile Application Single Sign-On: Improving Authentication for Public Safety First Responders (2nd Draft). National Institute of Standards and Technology. Retrieved October 2019 from: https://csrc.nist.gov/publications/detail/sp/1800-13/draft
- DHS, 2019. First Responder Authentication Credentials. DHS Science and Technology Directorate. Retrieved October 2019 from: https://www.dhs.gov/first-responder-authentication-credentials
- Federated ICAM Introduces New Capabilities for First Responders | May 2021. SIGNAL Magazine (afcea.org) https://www.afcea.org/content/federated-icam-introduces-new-capabilities-first-responders

- Northrop-Grumman, 2019. First Responder Authentication Credential (FRAC): Multi-Jurisdictional ID Authentication for First Responders. Retrieved October 2019 from: https://www.northropgrumman.com/Capabilities/IdentificationSystemsSolutions/FirstResponderAuthenticationCredential/Pages/default.aspx

Appendix B USE CASES

B.1 USE CASE INTRODUCTION

As described in the National Public Safety Telecommunications Council (NPSTC) June 2019 *"Public Safety Internet of Things (IoT) Use Case Report and Attributes,"* we are in the midst of a rapidly growing advanced technology environment in which a number of Internet-connected devices are capable of reporting environmental data, biometrics, tactical data, location, and a wealth of other information. Although many first responders are aware of public safety IoT, active planning to adopt the growing array of IoT tools is just beginning. This planning should incorporate an approach that begins with a self-assessment to determine a public safety agency's readiness level to receive, integrate, and implement these advance capabilities as well as consider the agency's mission, resources, policies, and governance. Once an agency has internally assessed their mission and mission needs, they should consult externally to validate and verify their internal assessment. These two activities align with the ISF Implementation Cycle's first two steps: Assess and Consult.

Appendix B is intended for both operational and technical public safety personnel and provides information on a sampling of representative use cases in public safety derived from prior NPSTC work. It illustrates how a use case can be disassembled into a sequence of actions from which system requirements can be derived. These use cases can be an exemplar for public safety agencies that are trying to address a similar use case and will serve as a starting point to develop baseline functional and technical requirements. These requirements can then be used by public safety agencies to perform a readiness level assessment, evaluate frameworks solutions/options, and as appropriate support iterative testing and evaluation. As this appendix evolves and matures, the content will also help technology developers and researchers better understand public safety's needs for IoT technologies and solutions, and will serve as a starting point for further investigation and research.

It should be noted that this appendix contains placeholders for material that is still under development, per this document version. The intent is to have this material finalized and added into the next version update.

B.2 METHODS

The use cases in this appendix are extracted from a set developed by the NPSTC[55]. NPSTC enlisted experts from public safety, government, and industry to develop this representative set, which can support the assessment of the evolution of IoT for public safety communications. The eight use cases address the following scenarios:

1) Routine Traffic Stop
2) Fire in a Single-Family Dwelling
3) Emergency Medical Response in a Home
4) Convenience Store Robbery
5) Traffic Accident Involving Hazardous Materials
6) Emergency Response in a Smart Building
7) Active Shooter
8) Response to an Extreme Weather Event

B.3 USE CASE DEVELOPMENT

The NPSTC Public Safety Internet of Things (PS IoT) Working Group developed the eight use cases to help ensure accurate assessment and consistency throughout the process. Each use case was based upon the following principles:

[55] https://www.npstc.org/download.jsp?tableId=37&column=217&id=4195&file=NPSTC_PSIoT_Use_Cases_Report_190616.pdf

- They are about a specific public safety **discipline** (law enforcement, fire, EMS, Emergency Communications Center (ECC)) or they may be a generic use case applicable to all entities.
- They are about a specific public safety **activity** (e.g., a traffic stop, a house fire, etc.) allowing us to identify unique IoT issues with these specific activities.
- They identify the different IoT **capabilities** needed to support public safety (e.g., video identification of a struggle).
- They should examine real time **tactical** uses of IoT data as well as **strategic** uses of IoT data for analysis, which allow for enhancements to the common operating picture, (e.g., situational awareness) and which create actionable intelligence.

B.4 ASSUMPTIONS

The following assumptions should be considered in regards to the NPSTC use cases:

- **Roles and Responsibilities:** It is assumed that each agency will define its own organizational structure and assign roles and responsibilities accordingly.
- **Life Cycle Issues:** Agencies will need to address issues of maintenance and long-term upgrade requirements. In addition, policies, procedures, and resource limitations (staff and budgets) also vary from agency to agency.
- **Data Storage:** Each agency has its own unique data storage requirements (technical, policies, governance, etc.) based on local laws and policy.
- **Credentialing:** Although Identity, Credential, and Access Management (ICAM) is a critical component of interoperability, it is not explicitly addressed in this appendix.
- **Personnel Resources:** Data and information come with a cost; it takes time to manage, retrieve, distribute, and interpret data. As the ability to store, retrieve, disseminate, and use data increases, the need for advanced decision support tools will increase dramatically. Workloads may be reduced somewhat by artificial intelligence-driven analytics, but these automated tools will also come with a cost.
- **Information Exchange:** Much of the information exchange identified in this document will involve content ownership and privacy considerations, which may dissuade organizations from sharing information. It is assumed that some potential solutions exist and that each agency will determine which solution(s) to adopt based on missions, resources, requirements, and budgets.
- **Emergency Communications Ecosystem:** The Ecosystem that comprises the emergency response system is dynamic, depending on the incident or planned event, and multi-directional because anyone can initiate emergency communications. Although the individual responsible for coordinating emergency communications varies across jurisdictions, regions, and organizations, having an established central point of contact is critical for progressing emergency communications capabilities.
- **Readiness Levels:** Many public safety agencies are not currently ready to receive or integrate some of the advanced solutions that are under development. Some agencies have legacy systems and limited resources (budget and personnel), and may not have the technical support required to manage and maintain some of the capabilities described in this document. Each public agency should self-assess to fully understand mission requirements and existing infrastructure and to determine readiness level to adopt and integrate new capabilities.

B.5 USE CASES

As previously described, the following eight uses cases were provided as representative background to begin documenting the functional and technological capabilities required for achieving the envisioned end-state for interoperability. Each use case includes:

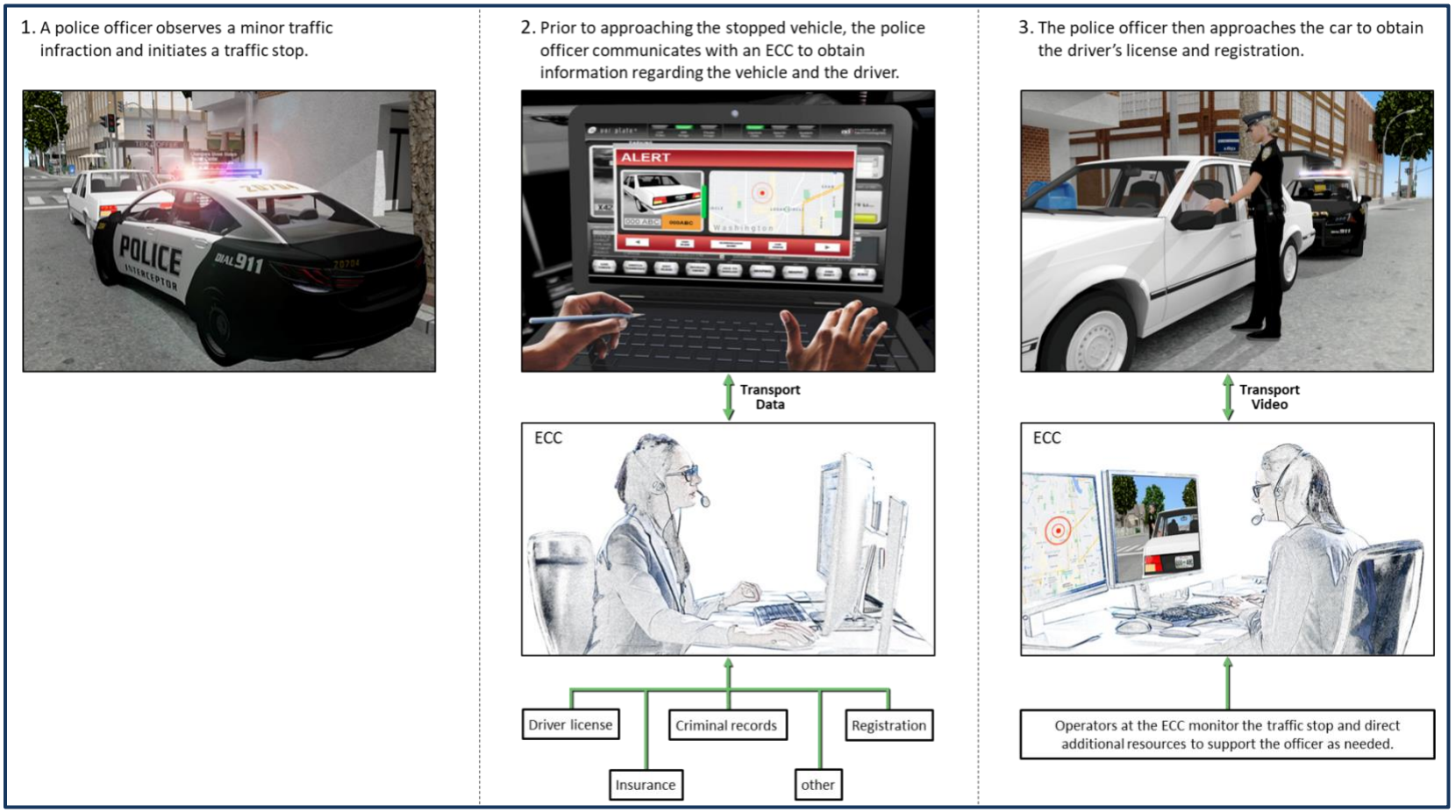
- Brief description of how the incident unfolds
- A storyboard that visually describes each of the incident steps
- A Concept of Operations that captures the major entities and their activities within an incident
- A table that details the specific steps and their associated stakeholders, mission, content, and transport entities
- Diagrams illustrating the information flows between stakeholders
- Technological capabilities needed

B.5.1 Use Case #1: Traffic Stop

B.5.1.1 Description

Use Case #1 describes a routine traffic stop in response to a moving violation. A police officer observes a minor traffic infraction and initiates a traffic stop. Prior to approaching the stopped vehicle, the police officer communicates with an ECC to obtain information regarding the vehicle. Information on the motor vehicle, along with criminal records on the vehicle and its owner, is obtained (e.g., registration, ownership, notification of any recent criminal activity involving the vehicle). Upon approaching the car and obtaining the driver's license and registration, the police officer obtains additional information. Operators at the ECC monitor the traffic stop and direct additional resources to support the officer as needed.

B.5.1.2 STORYBOARD



Apx Figure B-1: Use Case #1, Traffic Stop – Storyboard

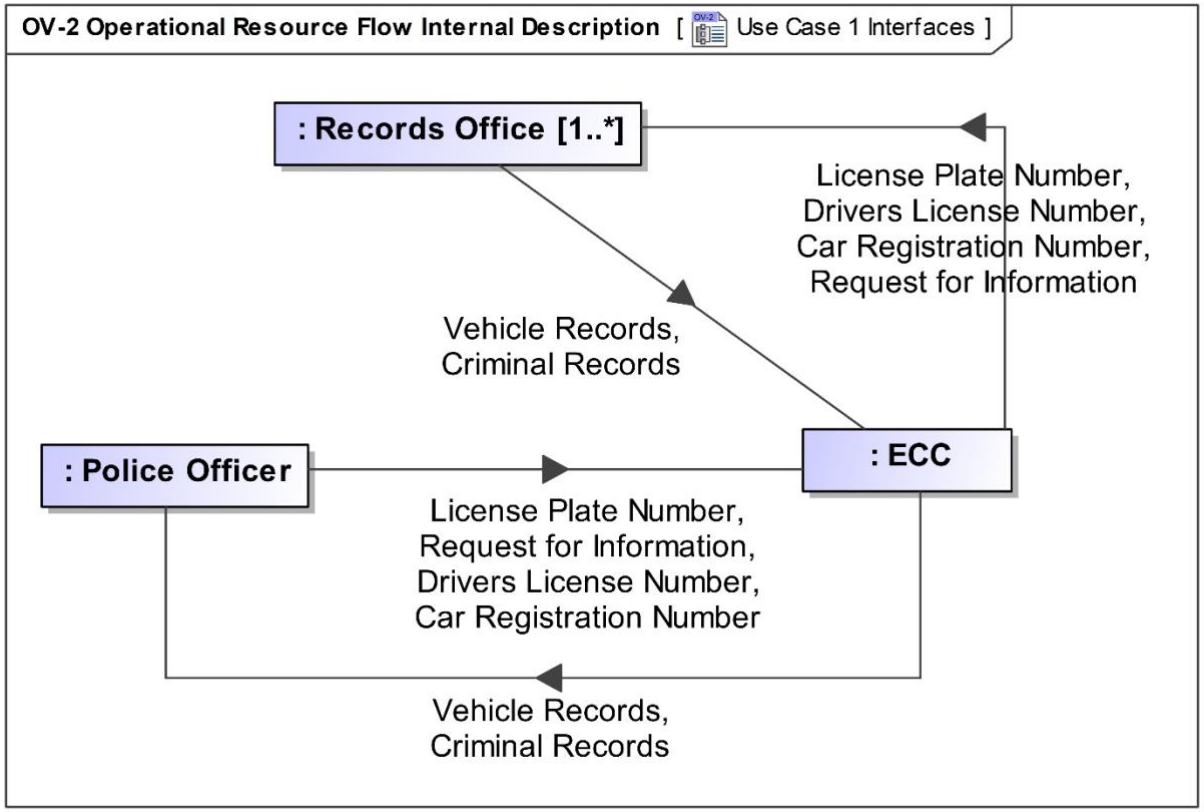
B.5.1.3 CONOPS

This section will be completed in the next revision.

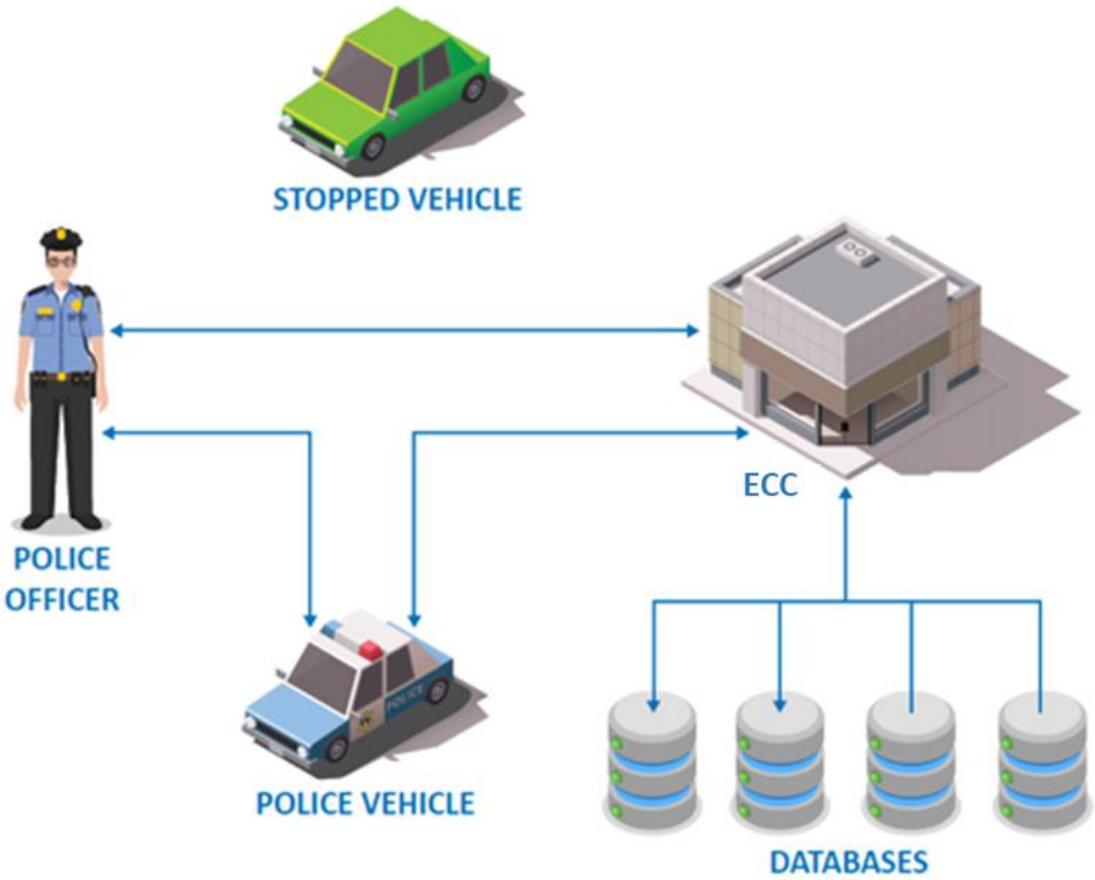
B.5.1.4 Timeline, Information Flow, and Required Technology Capabilities

Apx Table B-1: Use Case #1: Timeline versus Stakeholders, Mission, Conten,t and Transport

Step	Description	Stakeholders	Mission	Content	Transport
1	A police officer observes a minor traffic infraction and initiates a traffic stop. The policer officer is wearing a body camera and sensors that monitor health metrics.	• Police officer • Driver	Safely initiate traffic stop.	• Video • Sensor data	• LTE
2	Prior to approaching the stopped vehicle, the police officer communicates with an ECC to obtain information regarding the vehicle and the driver. The ECC sends relevant information on the vehicle and its owner (e.g., warrants, criminal records, registration, ownership, notification of any recent criminal activity involving the vehicle).	• Police Officer • Driver • ECC	Learn more about the vehicle and the driver and provide officer with relevant information.	• Voice/Audio • Text-based • Images • GPS	• Radio • LTE
3	The police offer then approaches the car to obtain the driver's license and registration. Operators at the ECC monitor the traffic stop, monitor the health of the officer, and direct additional resources to support the officer as needed.	• Police Officer • Driver • ECC	Ensure the safety of the police officer and other civilians.	• Video • Voice/Audio • Sensor data	• Radio • LTE



Apx Figure B-2: Use Case #1, Traffic Stop – Information Flow



Apx Figure B-3: Use Case #1, Traffic Stop

Apx Table B-2: Required Technical Capabilities – Traffic Stop

ISF Layer	Function	Capability
Data & Integration	Discovery & Data Exchange	• License plate scanning • Driver's License and Vehicle Registration Scanning • Physiological sensors - responders' health & safety • Body Worn Camera • Video/Text 911
Integration	Transport	• Fixed and wireless data networks including 5G and local area network, vehicle, and PAN that transport data to necessary networks and servers • Real-time transmission of live streaming video from UASs • Real-time transmission from body-worn sensors
Integration	Identity Management	• Secure credentialing to provide access to local databases including permit databases to identify businesses, weapons, or other key building information • Secure, need-to-know based access to non-local databases including out-of-state criminal and driving records
Integration	Analytics	• Decision support for rapid access, assessment, and dissemination of relevant data • Analytics to alert the call center of changes in the officer's status – health or safety
Presentation	Monitor	• Real-time monitoring of video and biometric data

B.5.2 Use Case #2: Dwelling Fire

B.5.2.1 Description

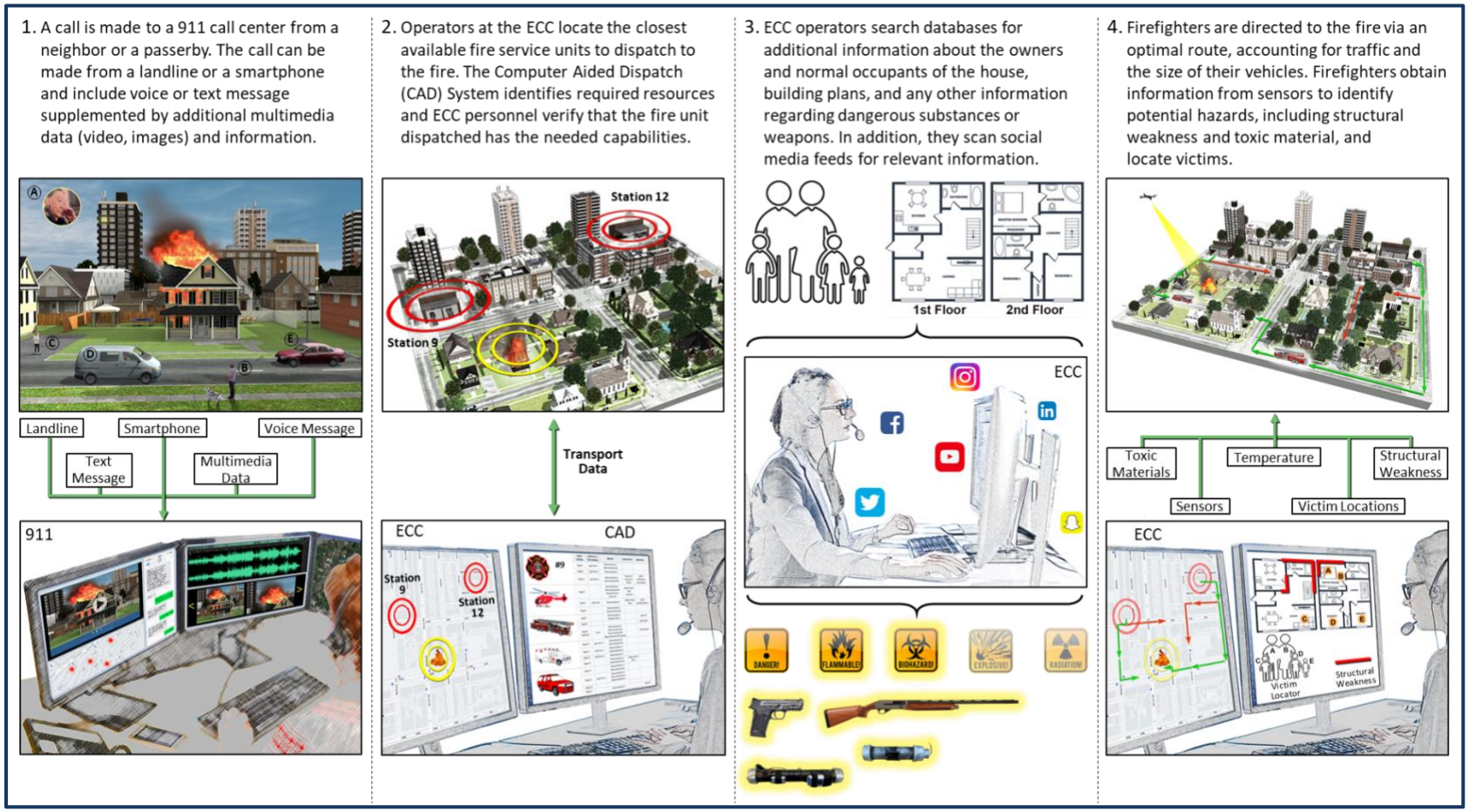
Use Case #2 describes a fire service response to a fire in a single-family dwelling. The use case begins with a call to a 911 call center from a neighbor or a passerby. The call can be made from a landline or a smartphone and include voice or text message supplemented by additional multimedia data (e.g., video, images) and information.

Upon receiving the 911 call, operators at the ECC locate the closest available fire service units to dispatch to the fire. The Computer Aided Dispatch (CAD) system identifies required resources, and ECC personnel verify that the fire unit dispatched has the needed capabilities. ECC operators search databases[56] for additional information about the owners and normal occupants of the house, building plans, and any other information regarding dangerous substances or weapons. In addition, they scan social media feeds for relevant information.

Firefighters are directed to the fire via an optimal route, accounting for traffic and the size of their vehicles. Firefighters obtain information en route and on location from unmanned sensors (e.g., UASs) to identify potential hazards, including structural weakness and toxic material in the atmosphere, and to locate victims. ECC operators monitor the response and dispatch additional resources as needed.

[56] *Searches can be automated based on received data.*

B.5.2.2 STORYBOARD



Apx Figure B-4: Use Case #2, Dwelling Fire – Storyboard

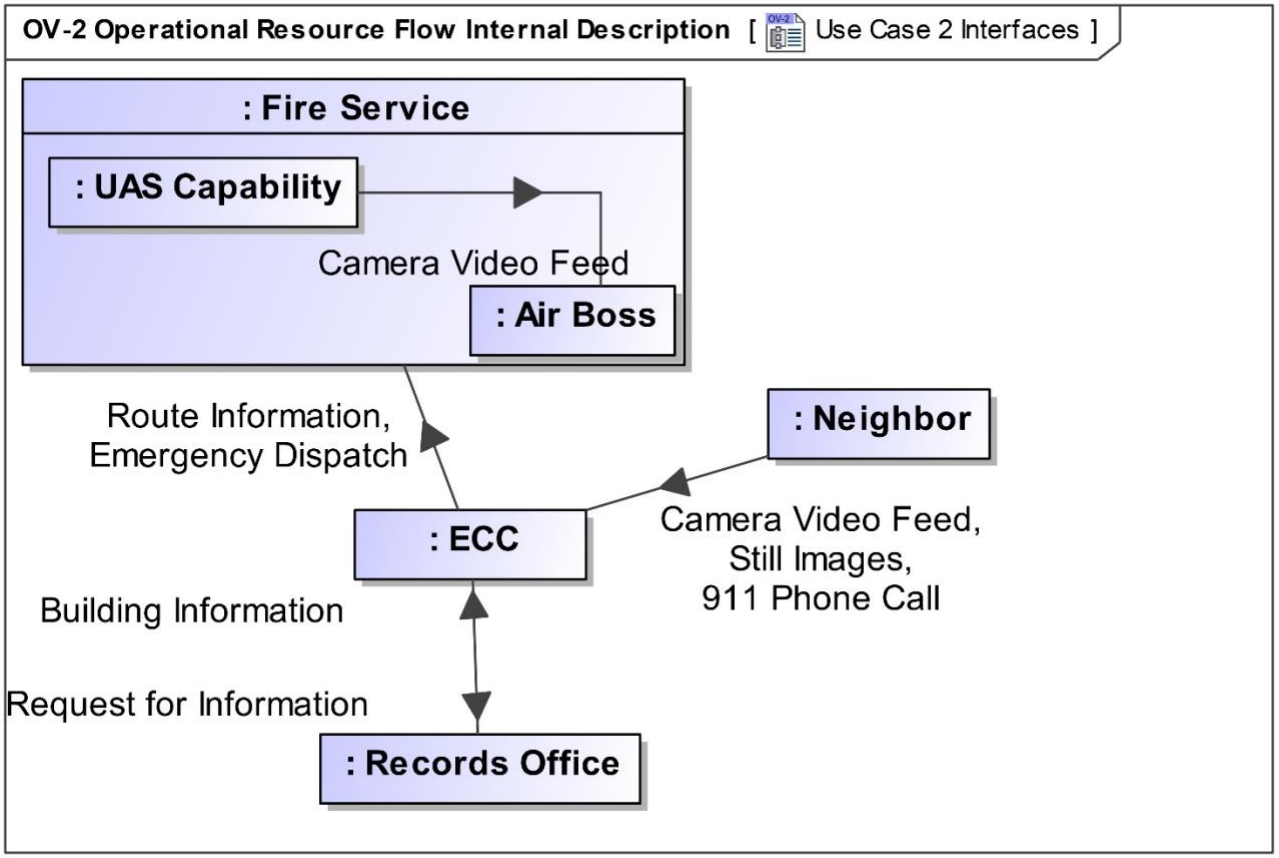
B.5.2.3 CONOPS

This section will be completed in the next revision.

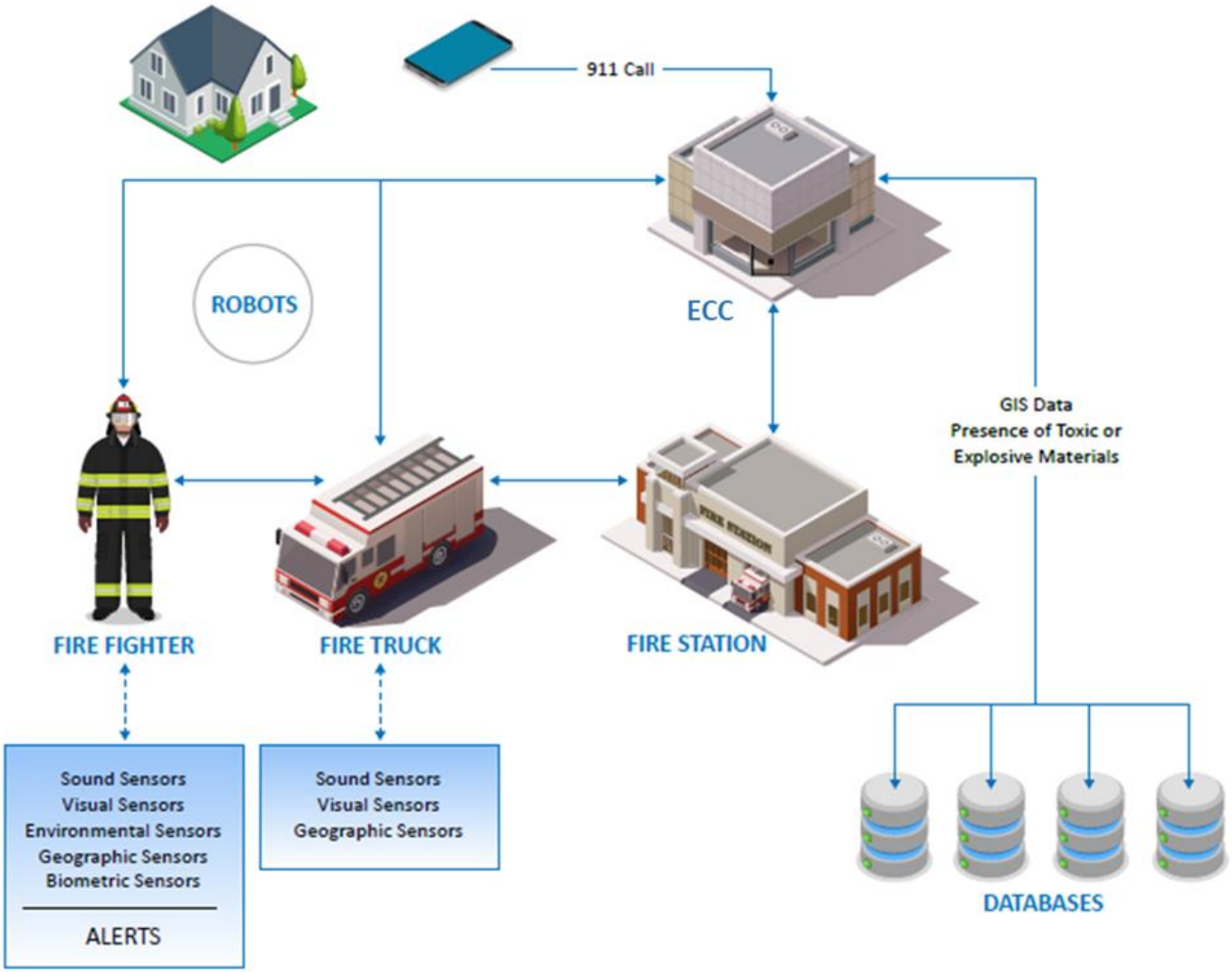
B.5.2.4 Timeline, Information Flow, and Required Technology Capabilities

Apx Table B-3: Use Case #2: Timeline versus Stakeholders, Mission, Content, and Transport

Step	Description	Stakeholders	Mission	Content	Transport
1	A call is made to a 911 call center from a neighbor or a passerby. The call can be made from a landline or a smartphone and include voice or text message supplemented by additional multimedia data (e.g., video, images) and information.	• Witnesses	Alert 911	• Voice/Audio • Video • Images • Text-based	• LTE • Landline
2	Upon receiving the 911 call, operators at the ECC locate the closest available fire service units to dispatch to the fire. The CAD system identifies required resources and ECC personnel verify that the fire unit dispatched has the needed capabilities.	• ECC • Firefighters	Gather information about the incident and dispatch the necessary public safety units.	• Voice/Audio • Video • Images • Text-based	• LTE
3	ECC operators search databases for additional information about the owners and normal occupants of the house, building plans, and any other information regarding dangerous substances or weapons. In addition, they scan social media feeds for relevant information.	• ECC • Firefighters	Gather supplemental information to provide to dispatch.	• Text-based • Social Media • Images	• LTE • Wi-Fi
4	Firefighters are directed to the fire via an optimal route, accounting for traffic and the size of their vehicles. Firefighters obtain information en route and on location from unmanned sensors (e.g., UASs) to identify potential hazards, including structural weakness and toxic material in the atmosphere, HAZMAT response protocols, and to locate victims. Additionally, this information is also sent back to the ECC for situational awareness.	• Firefighters	Safely route firefighter to location and provide up to date information.	• Sensor data • Video • Images • Text-based	• LTE
5	ECC operators monitor the response and dispatch additional resources as needed.	• ECC	Provide support to dispatch.	• Voice/Audio	• LTE • Radio



Apx Figure B-5: Use Case #2, Dwelling Fire – Information Flow



Apx Figure B-6: Use Case #2, Dwelling Fire

Apx Table B-4: Use Case #2: Required Technical Capabilities - Dwelling Fire

ISF Layer	Function	Capability
Data & Integration	Discovery & Data Exchange	• Physiological sensors - responders' health & safety • UAS live streaming video • Building sensors • Third party video surveillance systems • Body-worn sensors • Video/Text 911
Integration	Transport	• NG911 to support call, texts, video from scene • Fixed and wireless data networks including 5G and local area network, vehicle, and PAN that transport data to necessary networks and servers • Real-time transmission of live streaming video from UASs • Real-time transmission from body-worn sensors
Integration	Identity Management	• Secure credentialing to provide access to local databases including permit databases to identify businesses, weapons, or other key building information • Disseminate most recent building plans to responders on-scene
Integration	Analytics	• Determine most expeditious route using GIS capabilities • Decision support for rapid access, assessment and dissemination of relevant data • Sensor analytics to alert IC of changes in the on-scene responders' health and location
Presentation	Monitor	• Real-time monitoring of video and biometric data • Real-time monitoring of video from UASs and robots • Incident command makes informed decisions due to enhanced situational awareness

B.5.3 Use Case #3: Medical Emergency

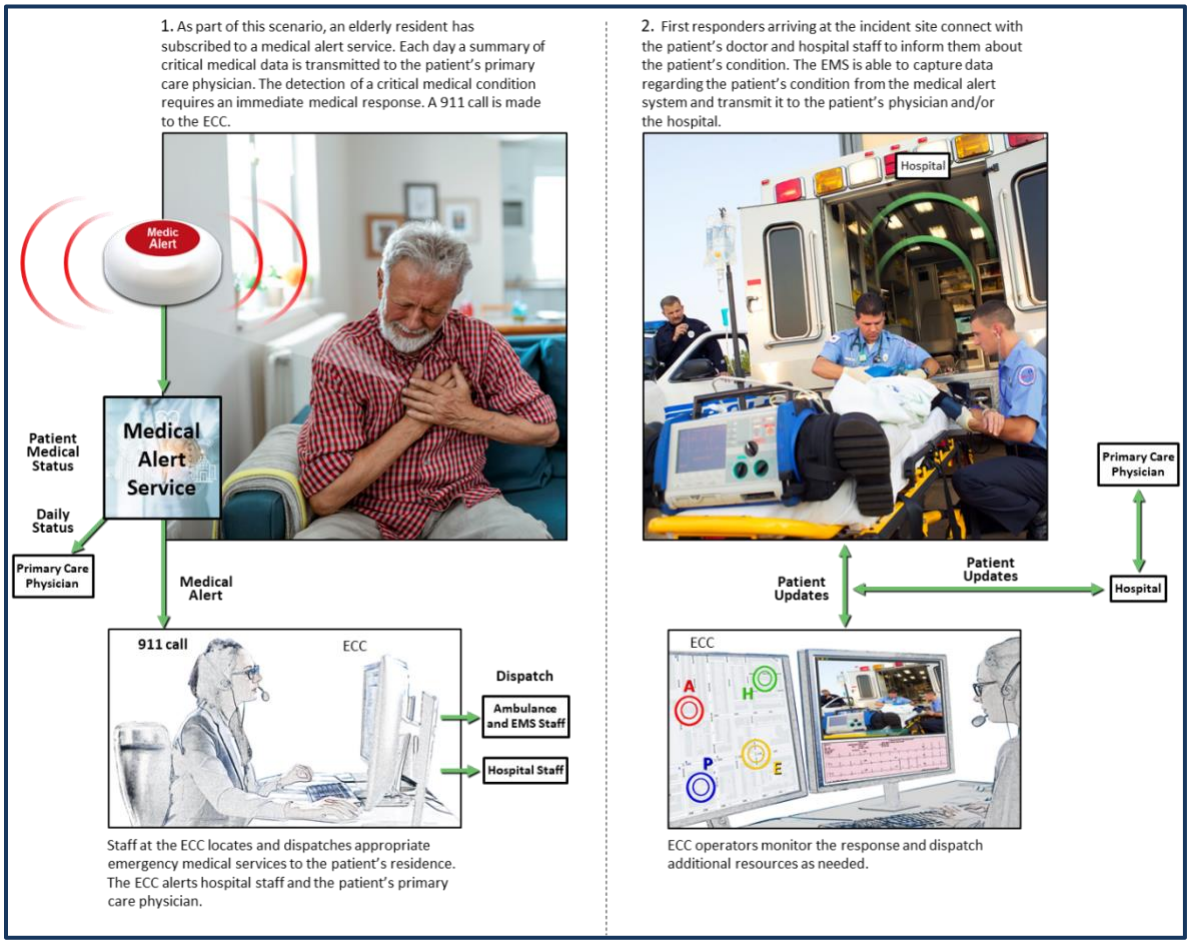
B.5.3.1 Description

Use Case #3 describes the response to a medical emergency in a home. As part of this scenario, an elderly resident has subscribed to a medical alert service. Each day a summary of critical medical data is transmitted to the patient's primary care physician.

Use Case #3 begins with the detection of a condition requiring an immediate medical response by the medical alerting system and a 911 call to the ECC (whether the alert is sent directly to the ECC by the medical alert system or whether an alert is provided to the medical alerting company or the patient's doctor is not addressed in this use case). Staff at the ECC locates and dispatches appropriate emergency medical services to the patient's residence. In addition, the ECC alerts hospital staff and the patient's primary care physician.

Finally, the communications architecture will provide first responders arriving at the incident site with connectivity to the patient's doctor, to hospital staff, and to information about the patient's condition from the medical alerting system. It will enable EMS to capture data regarding the patient's condition and transmit it to the patient's physician and/or the hospital.

B.5.3.2 STORYBOARD



Apx Figure B-7: Use Case #3, Medical Emergency – Storyboard

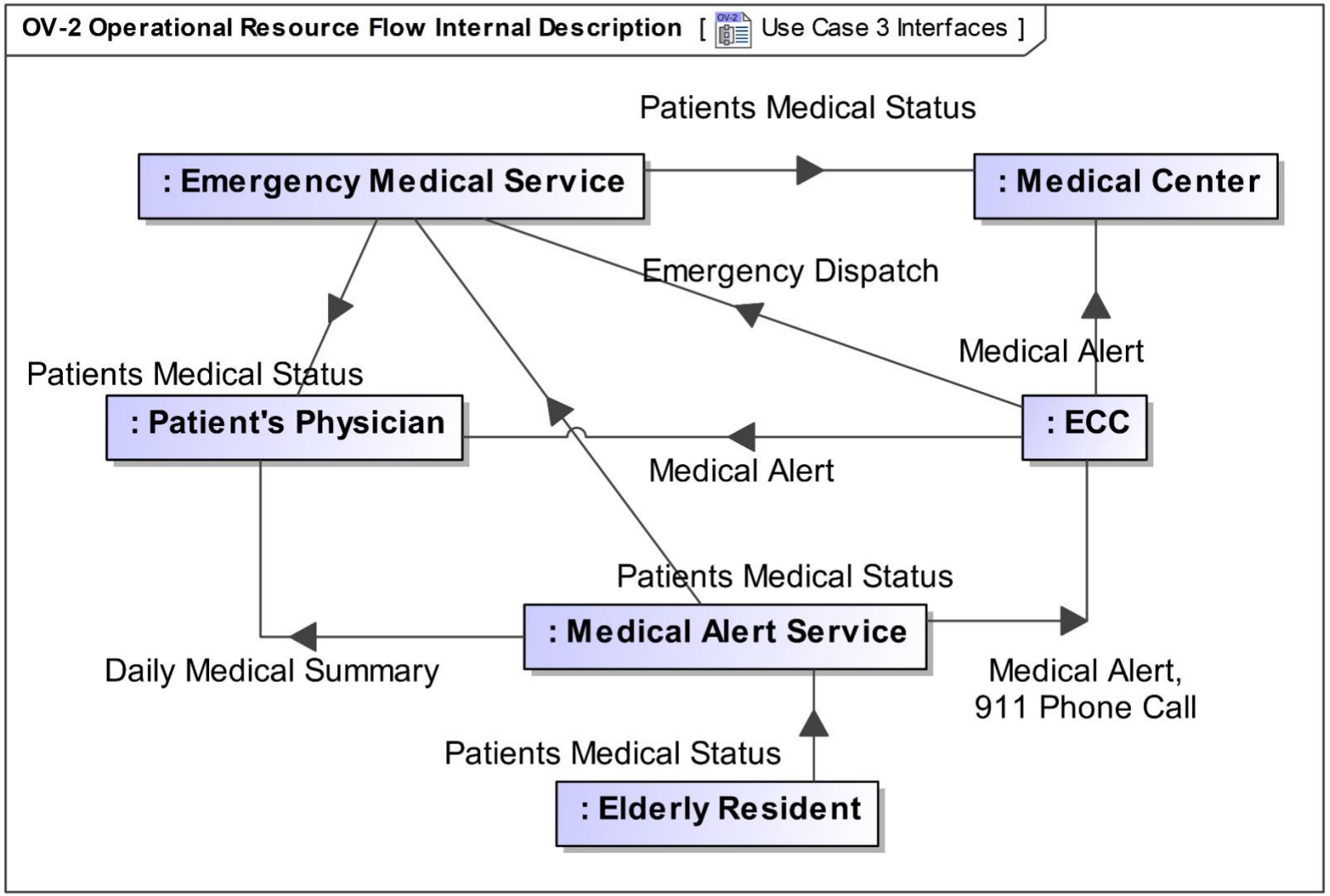
B.5.3.3 CONOPS

This section will be completed in the next revision.

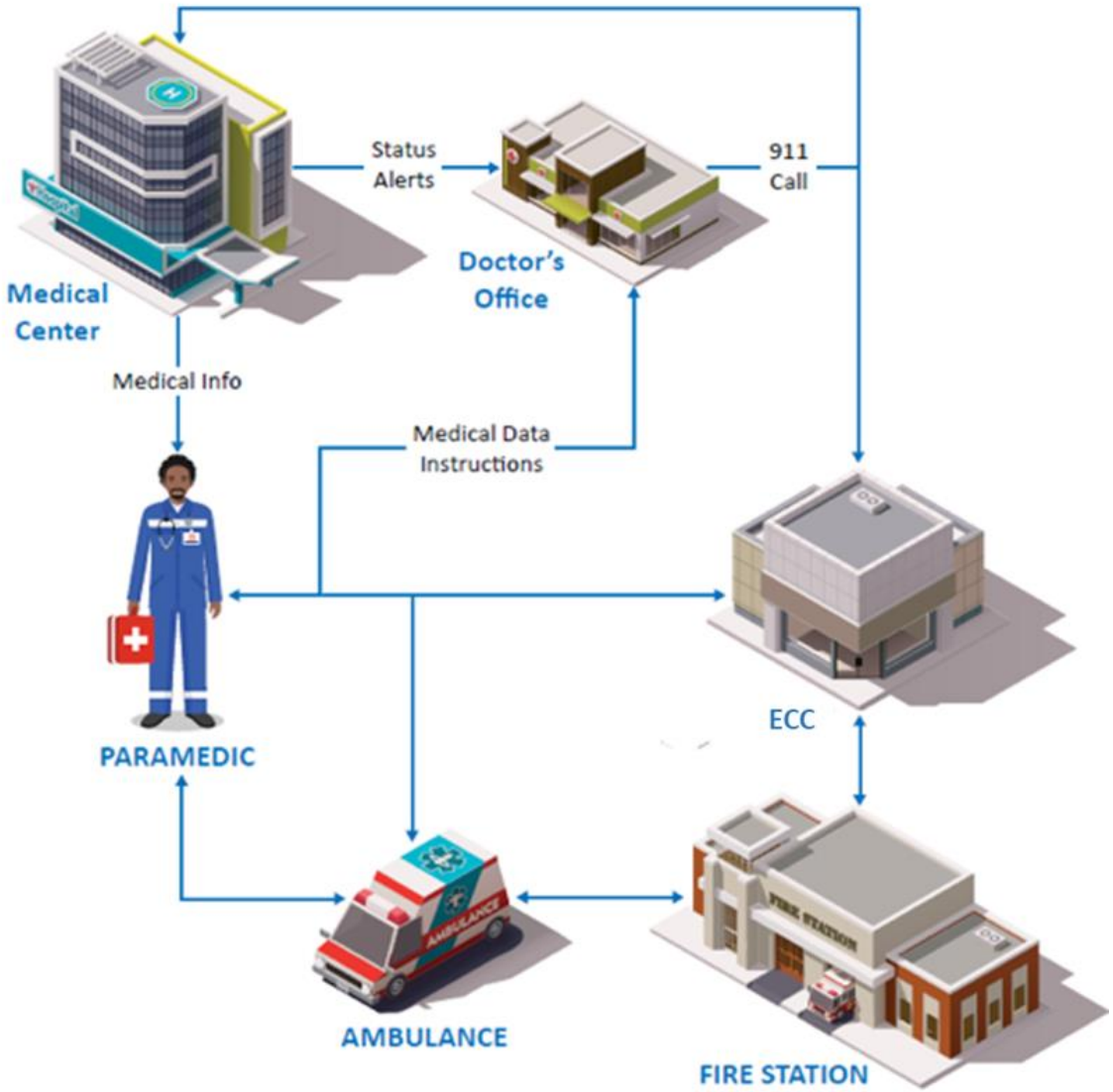
B.5.3.4 Timeline, Information Flow, and Required Technology Capabilities

Apx Table B-5: Use Case #3: Timeline versus Stakeholders, Mission, Content, and Transport

Step	Description	Stakeholder	Mission	Content	Transport
1	An elderly resident has subscribed to a medical alert service. Each day a summary of critical medical data is transmitted to the patient's primary care physician. The detection of a critical medical condition requires an immediate medical response. A 911 call is made to the ECC.	• Patient • Primary Care Physician • ECC • Medical Alert System Co	Acquire information about critical medical condition.	• Sensor data • Voice/Audio	• LTE • Wi-Fi • Bluetooth
2	Staff at the ECC locates and dispatches appropriate emergency medical services to the patient's residence.	• ECC • EMS	Rapidly dispatch emergency medical services.	• Voice/Audio • Text-based (Alerts)	• Radio • LTE
3	The ECC alerts hospital staff and the patient's primary care physician.	• ECC • Primary Care Physician	Inform hospital of critical information	• Voice/Audio	• LTE
4	First responders arriving at the incident site connect with the patient's doctor and hospital staff to inform them about the patient's condition. The EMS is able to capture data regarding the patient's condition from the medical alert system and transmit it to the patient's physician and/or the hospital.	• Primary Care Physician • Hospital Staff • EMS • Patient	Inform first responders of critical information.	• Voice/Audio • Text-based data • Sensor data	• LTE
5	ECC operators monitor the response and dispatch additional resources as needed.	• ECC	Provide support to dispatch.	• Voice/Audio	• LTE • Radio



Apx Figure B-8: Use Case #3, Medical Emergency – Information Flow



Apx Figure B-9: Use Case #3, Medical Emergency

Apx Table B-6: Use Case #3: Required Technical Capabilities - Medical Emergency

ISF Layer	Function	Capability
Data & Integration	Discovery & Data Exchange	• Sensors to measure critical patient health data
Integration	Transport	• Ability for EMS to communicate with health care providers • Device interoperability to enable the patient's medical monitoring system to interoperate with EMS equipment
Integration	Identity Management	• Secure credentialing to provide access to critical medical information
Integration	Analytics	• GIS to direct EMS to exact location of the patient by most expeditious route • CAD systems to rapidly locate and dispatch • Analytics to support health care decision making
Presentation	Monitor	• Real-time monitoring of physiological sensors • Enhanced data supports decision support regarding treatment and transport (e.g., criticality of patient determines appropriate treatment location)

B.5.4 Use Case #4: Convenience Store Robbery

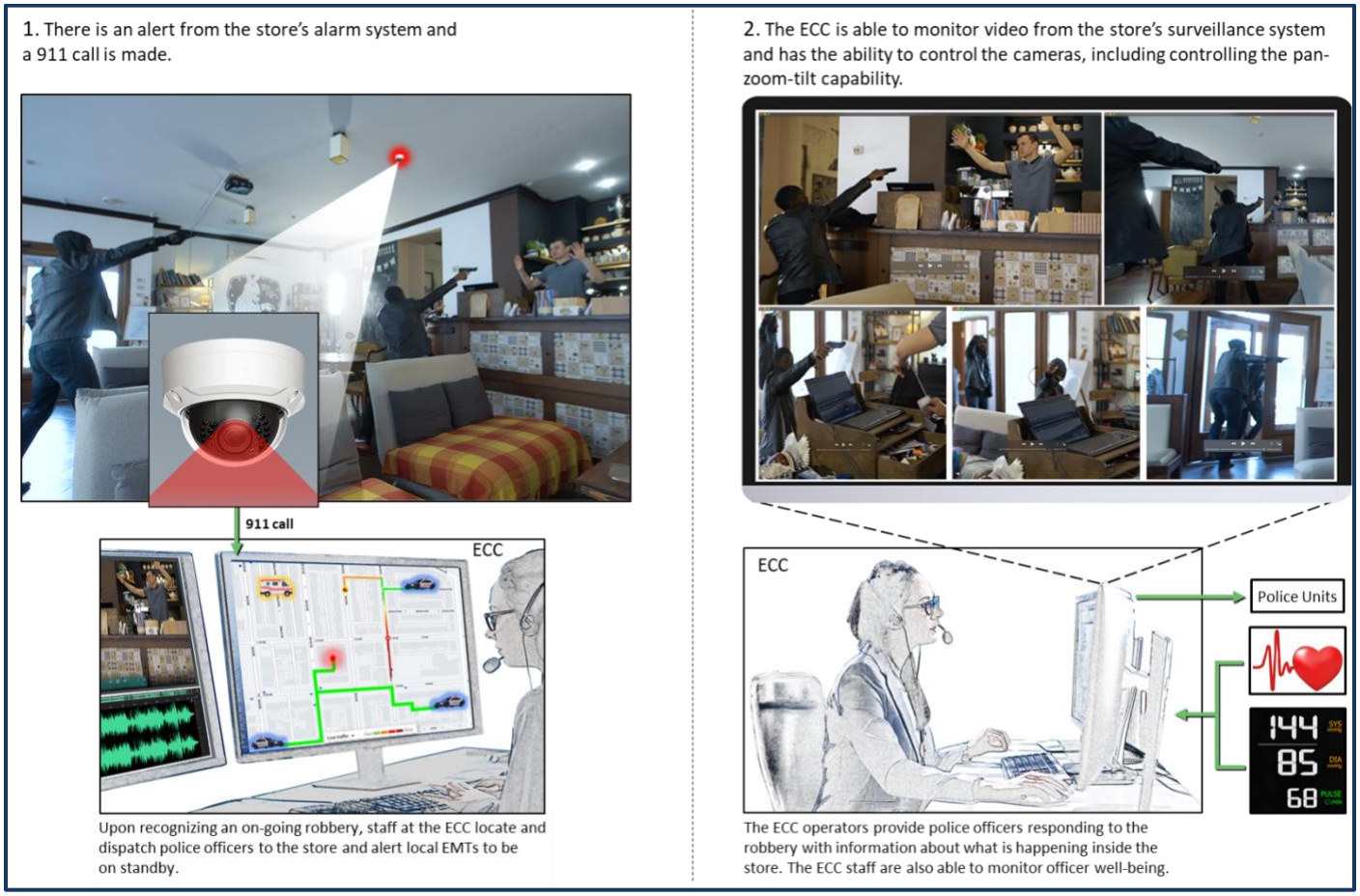
B.5.4.1 Description

Use Case #4 describes the response to a convenience store robbery. This use case begins with an alert from the store's alarm system or a 911 call. Upon recognizing an on-going robbery, staff at the ECC locate and dispatch police officers to the store.

The use case includes an ECC capability to monitor video from the store's surveillance system. It also describes the ECC having the ability to control the cameras, including controlling the pan-zoom-tilt capability.

Finally, the telecommunications architecture provides ECC operators the ability to provide police officers responding to the robbery with information about what is happening inside the store. It also provides ECC staff with the ability to monitor officer well-being.

B.5.4.2 STORYBOARD



Apx Figure B-10: Use Case #4, Convenience Store Robbery – Storyboard

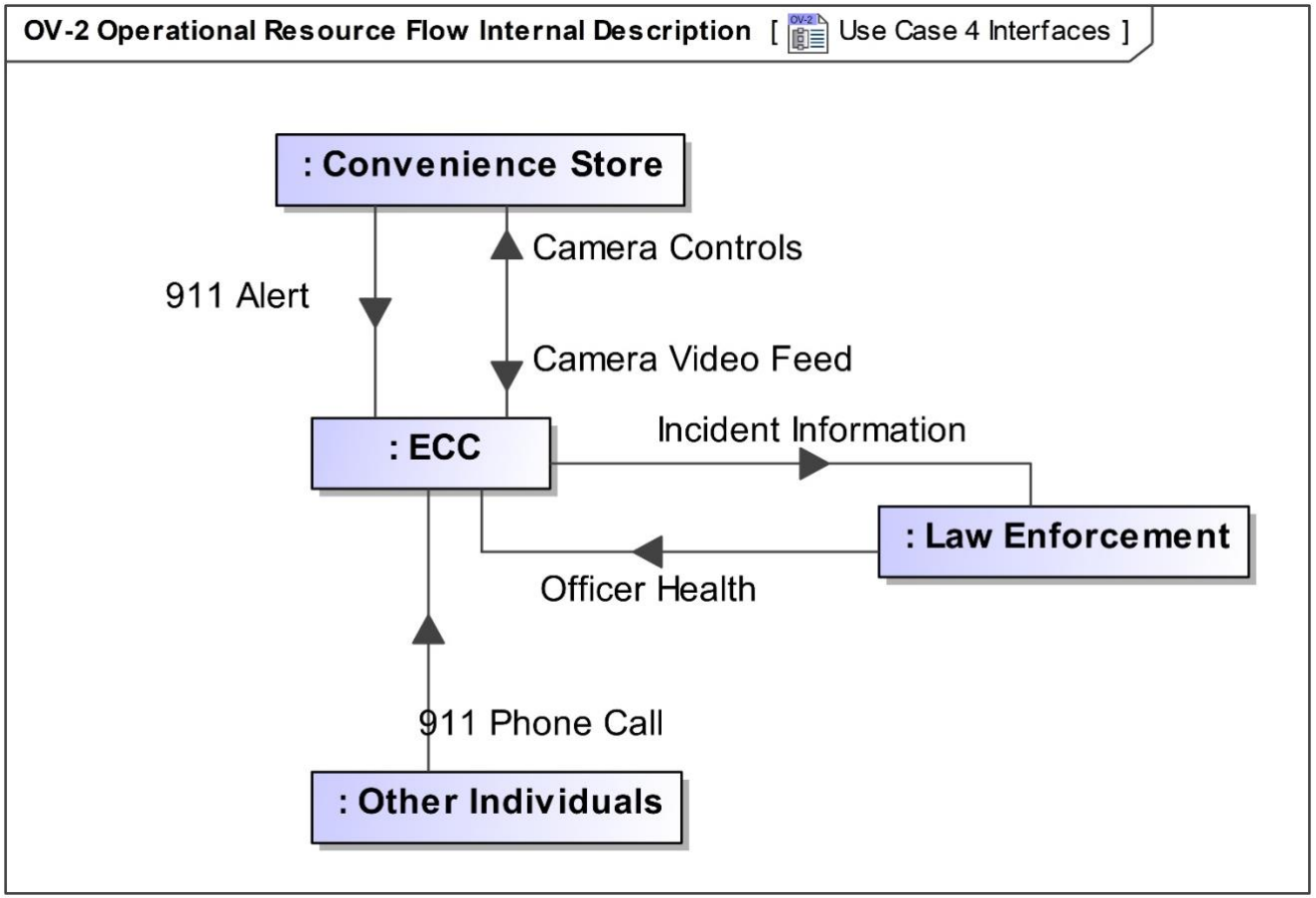
B.5.4.3 CONOPS

This section will be completed in the next revision.

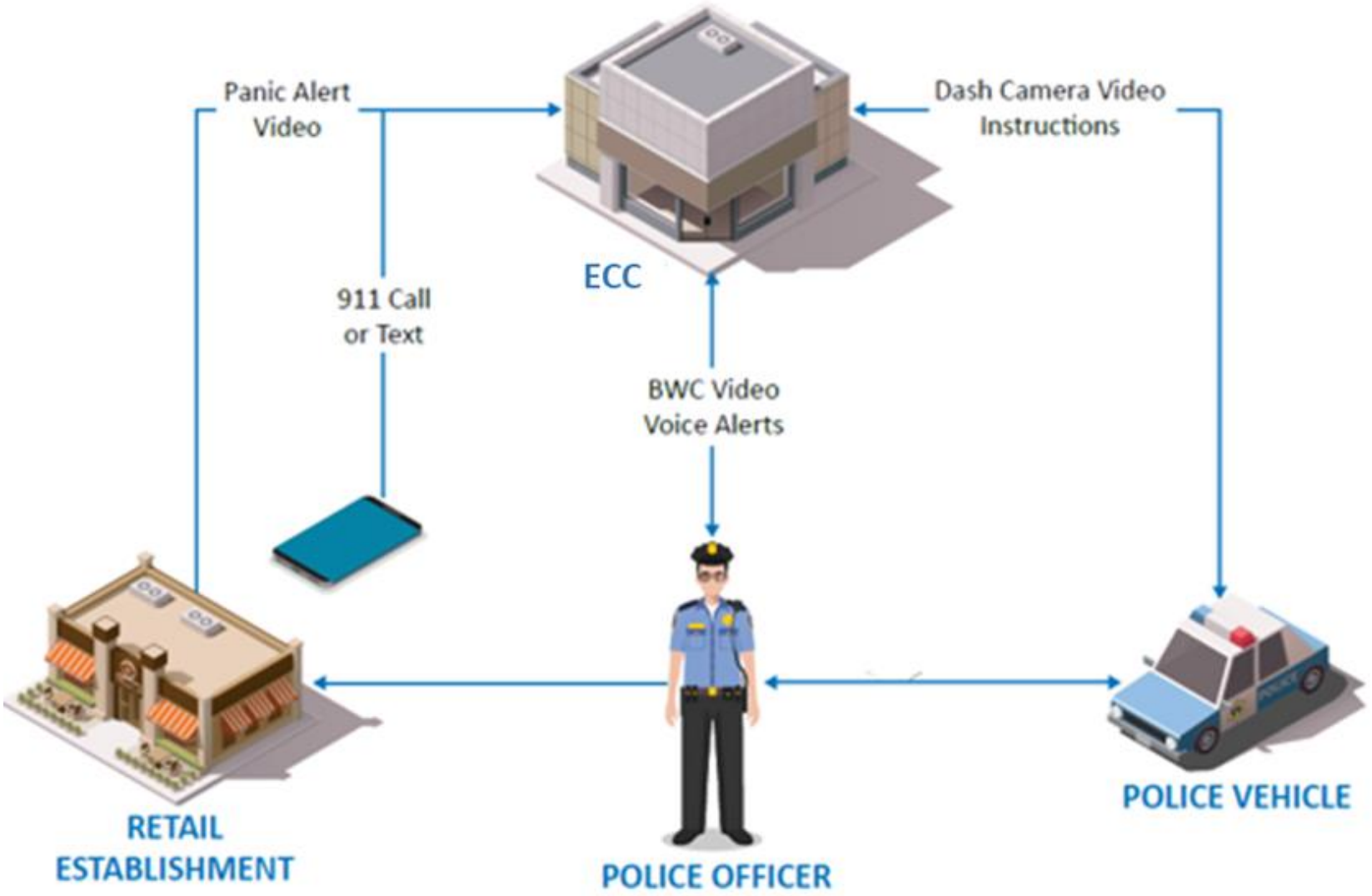
B.5.4.4 Timeline, Information Flow, and Required Technology Capabilities

Apx Table B-7: Use Case #4: Timeline versus Stakeholders, Mission, Content, and Transport

Step	Description	Stakeholder	Mission	Content	Transport
1	There is an alert from the store's alarm system and a 911 call is made. Additionally, bystanders and store customers call and text 911 with information.	• ECC • Alarm System Owners • Store Owner • Customers • Bystanders	Acquire information	• Voice/Audio • Text • Images	• LTE
2	Upon recognizing an on-going robbery, staff at the ECC locate and dispatch police officers to the store.	• ECC • Police Officer	Rapidly dispatch police officers to the location.	• Voice/Audio	• LTE • Radio
3	The ECC is able to monitor video from the store's surveillance system and has the ability to control the cameras, including controlling the pan-zoom-tilt capability. Upon arrival, the ECC monitors the health and safety of the police officers via body worn cameras and sensors.	• ECC • Alarm System Owners	Monitor the scene to provide additional resources as needed.	• Video • Sensor data	• LTE • Wi-Fi • Bluetooth
4	The ECC operators provide police officers responding to the robbery with information about what is happening inside the store.	• ECC • Police Officer	Relay critical information to onsite police officers in real time.	• Voice/Audio	• LTE • Radio
5	The ECC staff are also able to monitor officer well-	• ECC • Police Officer	Monitor police officers and provide assistance as needed.	• Sensor data • Video	• LTE • Wi-Fi • Bluetooth



Apx Figure B-11: Use Case #4, Convenience Store Robbery – Information Flow



Apx Figure B-12: Use Case #4, Convenience Store Robbery

Apx Table B-8: Use Case #4: Required Technical Capabilities – Convenience Store Robbery

ISF Layer	Function	Capability
Data & Integration	Discovery & Data Exchange	• Physiological sensors - responders' health & safety • UAS live streaming video • Third party video surveillance systems • Body Worn Cameras • Video/Text 911
Integration	Transport	• Store security system transmits alarm to the designated call center • NG911 to support call, texts, video from scene • Fixed and wireless data networks including 5G and local area network, vehicle, and PAN that transport data to necessary networks and servers • Real-time transmission of live streaming video • Real-time transmission from body-worn sensors
Integration	Identity Management	• Secure credentialing to provide access to local databases including permit databases to identify businesses, weapons, or other key building information • Disseminate most recent building plans to responders on-scene for entry options • Secure credentialing to provide access to criminal databases
Integration	Analytics	• Decision support for rapid access, assessment, and dissemination of relevant data • Sensor analytics to alert IC of changes in the on-scene responders' health and location
Presentation	Monitor	• Real-time monitoring of video and biometric data • Real-time monitoring of video from surveillance system • Incident command makes informed decisions due to enhanced situational awareness

B.5.5 USE CASE #5: TRAFFIC ACCIDENT WITH HAZMAT

B.5.5.1 DESCRIPTION

Use Case #5 describes a multi-service, multi-jurisdictional response to a traffic accident. The accident occurs on an Interstate Highway and involves a tractor trailer carrying hazardous material.

The use case begins with multiple calls to 911. Witnesses send text messages or smart phone video. ECC operators interview callers to assess the extent of the accident, including if emergency medical services will be required. Police, Fire, and EMS personnel are dispatched to respond to the incident. In addition, the ECC staff locate and dispatch resources to handle clean-up operations. ECC staff identify the truck cargo based upon license information and manifests.

UASs with cameras, as well as traffic surveillance cameras, provide additional views of the incident. ECC personnel review data from these sources.

Geographic Information System (GIS) capabilities are employed to locate required resources and to route first responders to the incident site. First responders arriving at the scene access additional information about the cargo (i.e. via the Wireless Information System for Emergency Responders[57] (WISER) application).

In this scenario, first responders coordinate to remove the disabled vehicle and to re-open the road. First responders on the scene are equipped with sensors to detect toxic materials in the air and on the ground.

Due to the potential state and regional impact of this incident – closure of the interstate for an extended period of time could have significant economic implications – on scene commanders provide status to state and possibly federal agencies on progress.

Communications and alerts are sent to the public to route traffic away from the crash site via local television and radio broadcasts and via highway signs.

B.5.5.2 STORYBOARD

The graphics for this section will be completed in the next revision.

Apx Figure B-13: Use Case #5, Traffic Incident with Hazmat – Storyboard [Figure place holder]

B.5.5.3 CONOPS

This section will be completed in the next revision.

---

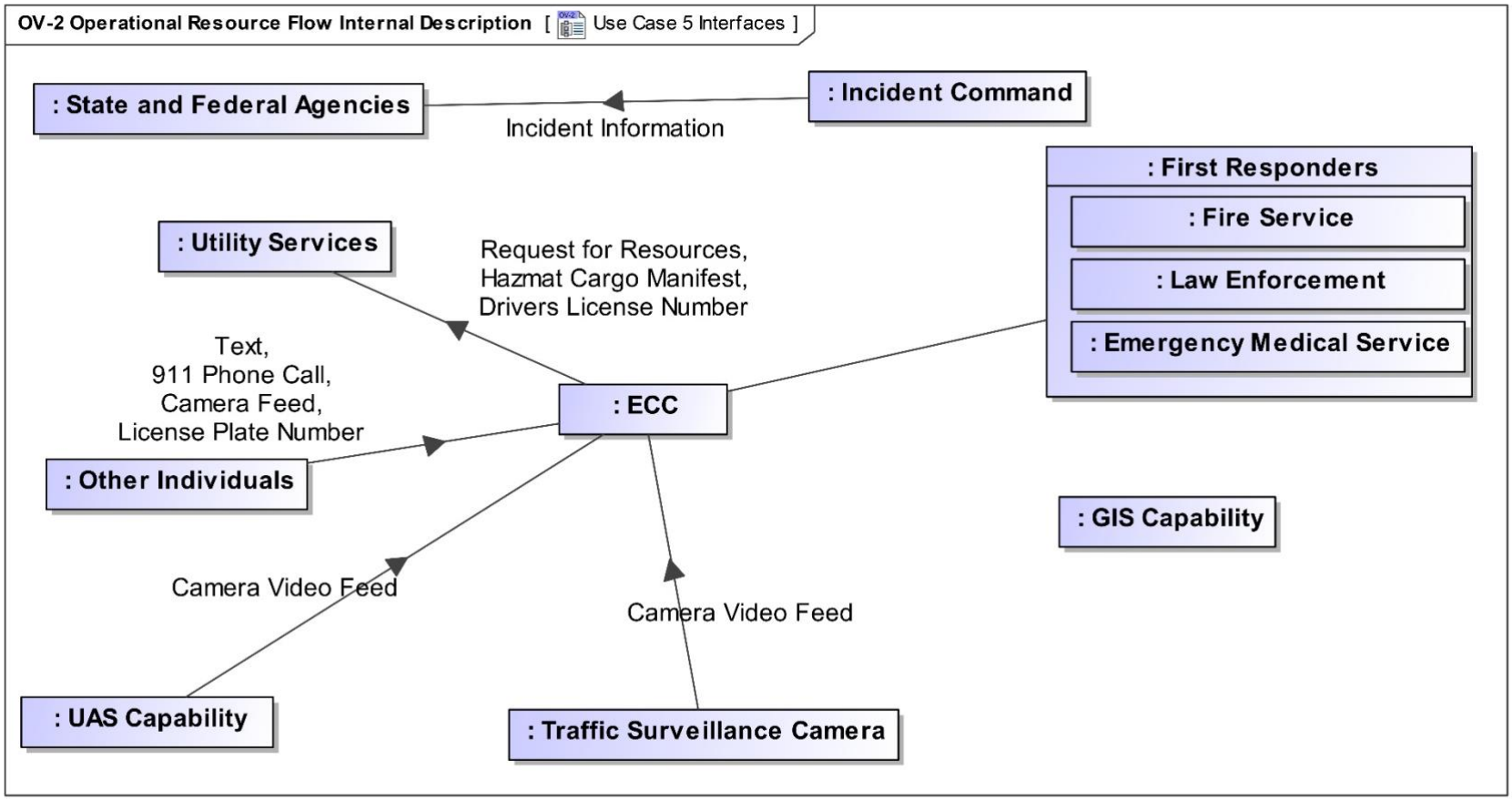
[57] ***WISER*** *is a system designed to assist emergency responders in hazardous material incidents. WISER provides a wide range of information on hazardous substances, including substance identification support, physical characteristics, human health information, and containment and suppression advice.*

B.5.5.4 Timeline, Information Flow, and Required Technology Capabilities

Apx Table B-9: Use Case #5: Timeline versus Stakeholders, Mission, Content, and Transport

Step	Description	Stakeholder	Mission	Content	Transport
1	An accident occurs on an Interstate Highway and involves a tractor trailer carrying hazardous material. There are multiple calls to 911. Witnesses send text messages or smart phone video. ECC operators interview callers to assess the extent of the accident, including if emergency medical services will be required.	• Witnesses • ECC	Acquire information about the incident.	• Voice/Audio • Text-based • Images	• LTE
2	Police, Fire, and EMS personnel are dispatched to respond to the incident.	• Police • Fire • EMS	Rapidly dispatch necessary services to the location.	• Voice/Audio • Text-based (Alerts)	• Radio • LTE
3	The ECC staff locate and dispatch resources to handle clean-up operations. ECC staff identify the truck cargo based upon license information and manifests.	• ECC	Help enable remediation of the incident.	• Voice/Audio • Text-based (Alerts)	• Radio • LTE
4	UASs with cameras, as well as traffic surveillance cameras, provide additional views of the incident. The ECC personnel review data from these sources.	• ECC • Police • Fire • EMS • UAS operators	Monitor incident and provide assistance as needed.	• Video • Voice/Audio • Images	• LTE • Fiber optic cable
5	GIS capabilities are employed to locate required resources and to route first responders to the incident site.	• GIS System Owners • Police • Fire • EMS	Route first responders to incident rapidly and safely.	• GPS • Voice/Audio	• Satellite • Radio • LTE
6	First responders arriving at the scene access additional information about the cargo (i.e. via the Wireless Information System for Emergency Responders (WISER) application). First responders contact the owners of the vehicle to learn more about the contents and quantities.	• Police • Fire • EMS • Vehicle owners	Learn more about contents of the cargo to respond accordingly.	• Text-based • Voice./Audio	• LTE

7	First responders on the scene are equipped with sensors to detect toxic materials in the air and on the ground.	• Police • Fire • EMS	Monitor environmental conditions and report data.	• Sensor data	• Sensor specific
8	Communication and alerts to the public to route traffic away from the crash site via local television and radio broadcasts and via highway signs.	• Civilians	Alert public of incident.	• Text-based	• LTE
9	Due to the potential state and regional impact of this incident – closure of the Interstate for an extended period could have significant economic implications – on scene commanders provide status to state and possibly federal agencies on progress.	• Police • Fire • EMS • State Agencies • Federal Agencies	Provide key decision makers with critical information.	• Voice/Audio • Text-based	• LTE



Apx Figure B-14: Use Case #5, Traffic Incident with Hazmat – Information Flow

Apx Table B-10: Use Case #5: Required Technical Capabilities – Traffic Incident with HAZMAT

ISF Layer	Function	Capability
Data & Integration	Discovery & Data Exchange	• Physiological sensors - responders' health & safety • Sensors on responders' gear to detect and identify HAZMAT • UAS live streaming video • Third party video surveillance systems • Body Worn Cameras • Video/Text 911
Integration	Transport	• Public safety agencies transmit instructions to the public via broadcast media and through electronic roadside signs • Incident command provides coordination to first responders • Communications with state and federal agencies for situational awareness and resource coordination • Fixed and wireless data networks including 5G and local area network, vehicle, and PAN that transport data • Real-time transmission of live streaming video from UAS • Real-time transmission from body-worn sensors
Integration	Identity Management	• Access to third party traffic cameras • Access to third party databases to identify truck cargo
Integration	Analytics	• Decision support for rapid access, assessment and dissemination of relevant data • Sensor analytics to alert IC of changes in the on-scene responders' health and location • GIS to route emergency responders to and to re-route public away from crash site
Presentation	Monitor	• Real-time monitoring of video and biometric data • Real-time monitoring of video from surveillance system • Incident command makes informed decisions due to enhanced situational awareness

B.5.6 Use Case #6: Large Building Fire

B.5.6.1 Description

Use Case #6 describes the response to a fire in a large building with a comprehensive 5G enabled sensing system. The use case begins with an alert from the building alarm system. Operators at the ECC receive calls from nearby citizens and people in the building via landline or cellular. Some smart phone users provide images, videos, and text.

Upon receiving the calls, operators at the ECC locate the closest available fire service units for dispatch. Automated capabilities allow them to quickly access databases for additional information about the owners and normal occupants of the building, building plans, and any other critical information such as criminal activity or the presence of hazardous materials. ECC personnel access information from the building's control systems to include video, heat and atmospheric sensors, and monitoring.

Firefighters responding are directed to the location via an optimal route, accounting for traffic and the size of their vehicles. They obtain information from unmanned sensors (e.g., UASs) to identify potential hazards, including structural weakness and toxic material in the atmosphere, and to locate victims.

IC monitors the first responders' safety via physiological sensors that display vital signs to the Medical Chief and IC's tablets. The IC is also able to see alerts from the chemical sensors attached to the firefighter's gear as well as monitor the location of teams via geolocation devices for accountable checks.

B.5.6.2 Storyboard

The graphics for this section will be completed in the next revision.

Apx Figure B-15: Use Case #6, Large Building Fire – Storyboard [Figure place holder]

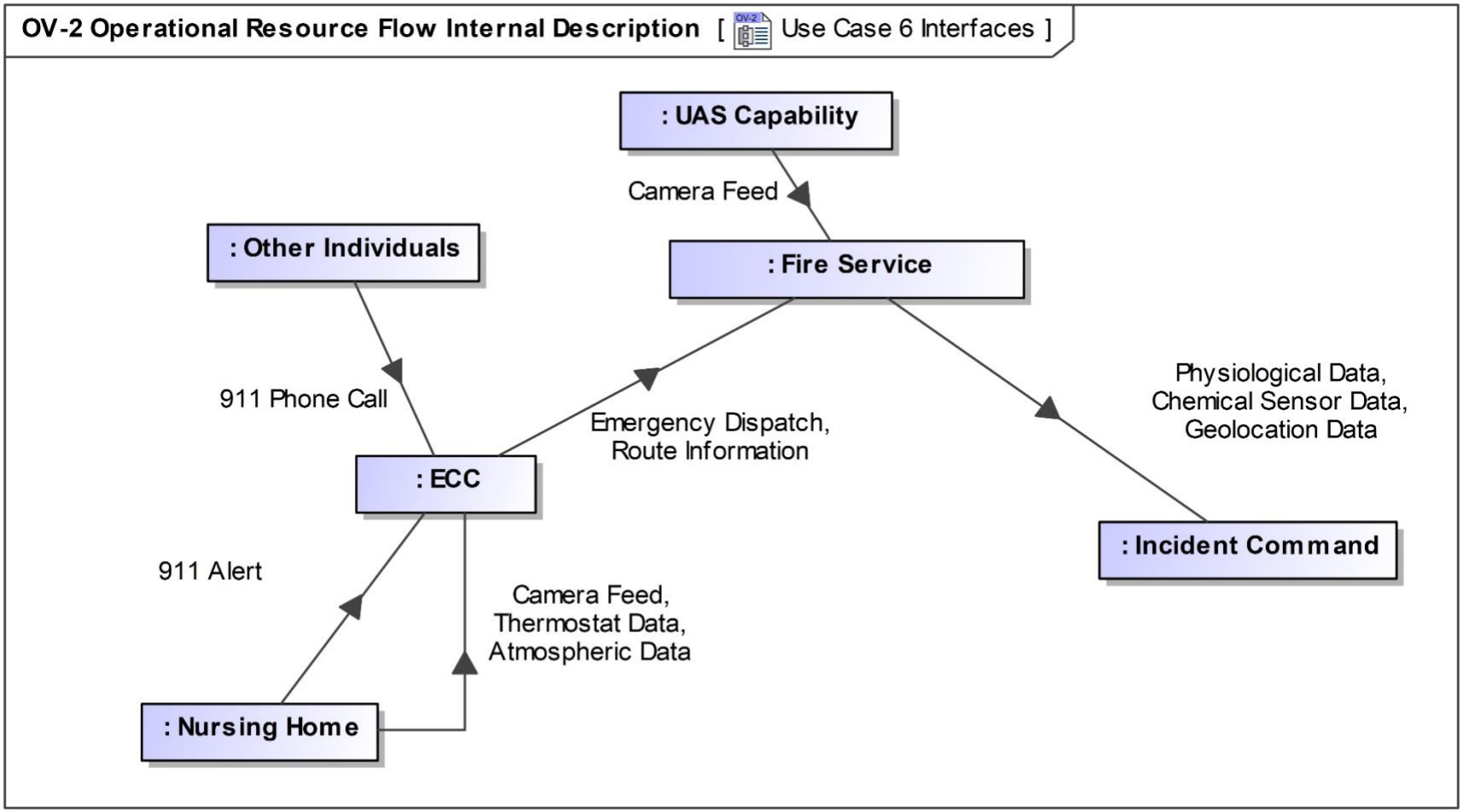
B.5.6.3 CONOPS

This section will be completed in the next revision.

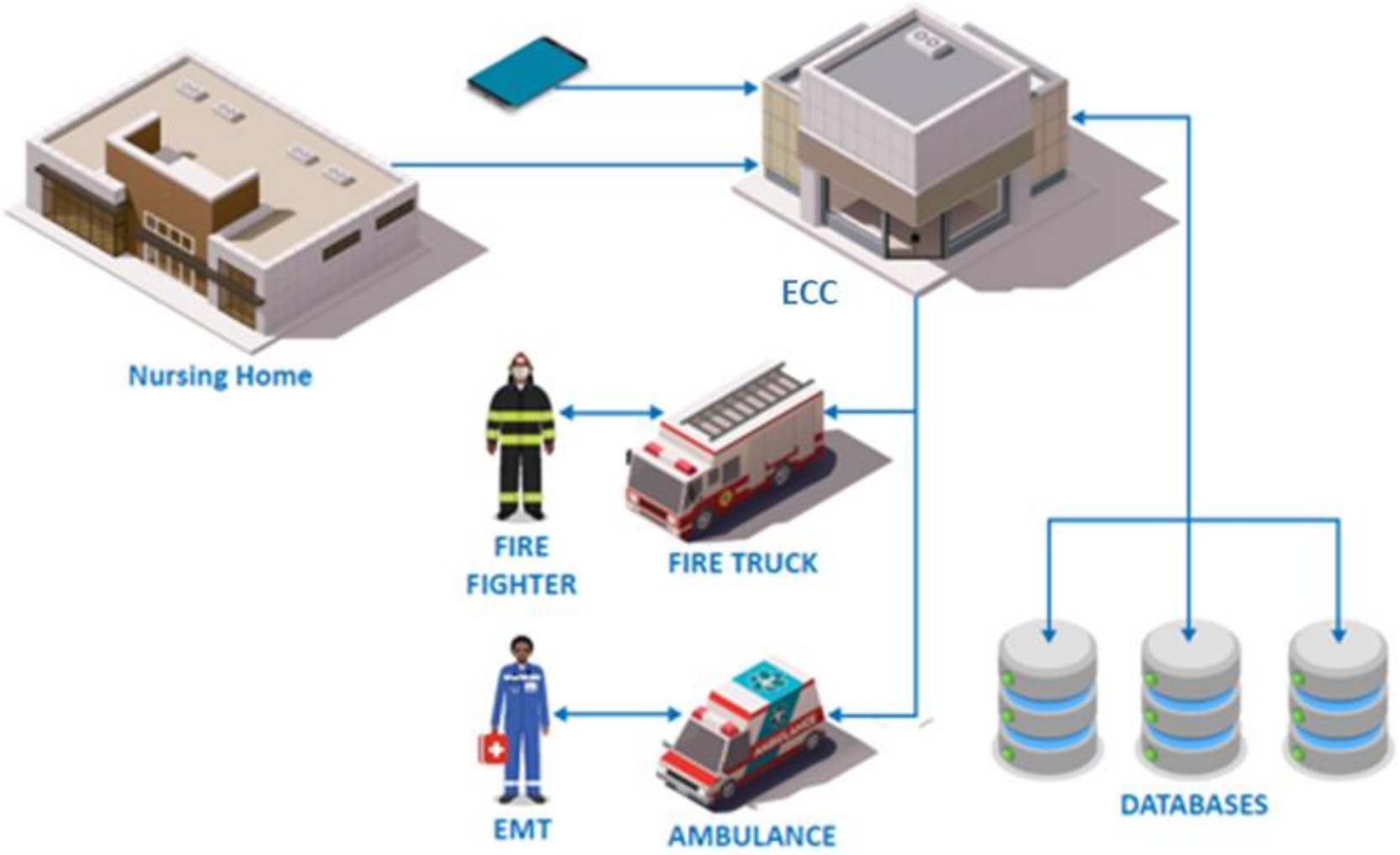
B.5.6.4 Timeline, Information Flow, and Required Technology Capabilities

Apx Table B-11: Use Case #6: Timeline versus Stakeholders, Mission, Content, and Transport

Step	Description	Stakeholder	Mission	Content	Transport
1	There is an alert from the building alarm system. Operators at the ECC receive calls from nearby citizens and people in the building via landline or cellular. Some smart phone users provide images, videos, and text.	• Citizens • ECC • Alarm System Owner • Building Owner	Acquire information about the incident.	• Video/Audio • Images • Text-based	• LTE • Landline
2	Upon receiving the calls, operators at the ECC locate the closest available fire service units for dispatch. Automated capabilities allow them to quickly access databases for additional information about the owners and normal occupants of the building, building plans, and any other critical information such as criminal activity or the presence of hazardous materials.	• ECC • Firefighters • Building Occupants	Dispatch fire units and gather critical information.	• Voice/Audio • Text-based	• Radio • LTE
3	ECC personnel access information from the building's control systems to include video, heat and atmospheric sensors, and monitoring.	• ECC	Access smart building sensors to analyze data.	• Video • Sensor data	• LTE • Wi-Fi • Sensor • specific
4	Firefighters responding are directed to the location via an optimal route, accounting for traffic and the size of their vehicles. They obtain information from unmanned sensors (e.g., UASs) to identify potential hazards, including structural weakness and toxic material in the atmosphere, and to locate victims.	• Firefighters	Equip onsite firefighters with critical information about the incident.	• Video	• Satellite • RF
5	IC monitors the first responders' safety via physiological sensors that display vital signs to the Medical Chief and IC's tablets. The IC is also able to see alerts from the chemical sensors attached to the firefighter's gear as well as monitor the location teams via geolocation devices for accountable checks.	• Firefighters	Monitor the safety of on scene responders.	• Sensor data • GPS	• Satellite • LTE • Bluetooth



Apx Figure B-16: Use Case #6, Large Building Fire – Information Flow



Apx Figure B-17: Use Case #6, Large Building Fire

Apx Table B-12: Use Case #6: Required Technical Capabilities – Large Building Fire

ISF Layer	Function	Capability
Data & Integration	Discovery & Data Exchange	• Third party video surveillance system • Smart sensors in building provide information regarding temperature, toxicity, and structural integrity of the building • Physiological sensors - responders' health & safety • Sensors on responders' gear to detect and identify HAZMAT • UAS live streaming video • Third party video surveillance systems • Body Worn Cameras
Integration	Transport	• Incident command provides coordination to first responders • Building smart sensor system transmits fire alarm to ECC • NG911 service supports calls, text, and multimedia data from the incident scene • UAS sensors provide live streaming video • Incident command centers provide coordination to first responders responding to the fire
Integration	Identity Management	• Access to third party traffic cameras and smart sensor grid • Access to information about building residents, businesses
Integration	Analytics	• Decision support for rapid access, assessment, and dissemination of relevant data • Sensor analytics to alert IC of changes in the on-scene responders' health and location • GIS to route emergency responders to and to re-route public away from crash site
Presentation	Monitor	• Real-time monitoring of video and biometric data • Real-time monitoring of video from surveillance system • Incident command makes informed decisions due to enhanced situational awareness

B.5.7 Use Case #7: Active Shooter

B.5.7.1 Description

Use Case #7 describes a public safety response to a shooting in a school. Key capabilities exercised in this scenario include coordination between multiple services and multiple jurisdictions and the use of third-party data, including school records and video streams from school surveillance cameras. Critical issues include negotiating privileges between law enforcement and the school district.

The use case begins with either an alarm from the school or a 911 call. The ECC receives multiple calls from students and staff inside the school, and the ECC staff collect as much useful information as possible from those calls. At the same time, the ECC staff direct resources to the school, including police and EMS, and coordinate with other ECCs for support from nearby jurisdictions.

The ECC assesses available information such as blueprints, entry points, etc. Video streams from cameras inside the school are used to help locate the shooter and detect any additional devices planted within the school. Video feeds are made available to the local bomb squad to enable them to assess potential danger. Incident command monitors responders' physiological sensors.

As responders arrive at the school, they coordinate with the School Resource Officer (SRO) who has been on scene. ECC personnel direct them to safe entry points and to the shooter's location. They provide as much information as possible on the shooter (or shooters), weapons involved, potential explosive devices, etc. Decision aids associated with the video feeds from the school provide ECC staff with information and potential blind spots.

Incident command is established and is being provided with video feeds. Rescue Task Force (RTF) units and additional EMS personnel have set up a triage, treatment, and transport area (T-3). IC receives notification from the SRO to have RTFs enter at a designated safe location to retrieve injured victims. ECC staff continue to scan the building via video for injured or hiding students and staff. EMS use their handheld devices to transmit images of the injured to Emergency Departments (EDs) to help prepare for surge.

B.5.7.2 Storyboard

The graphics for this section will be completed in the next revision.

Apx Figure B-18: Use Case #7, Active Shooter – Storyboard [Figure place holder]

B.5.7.3 CONOPS

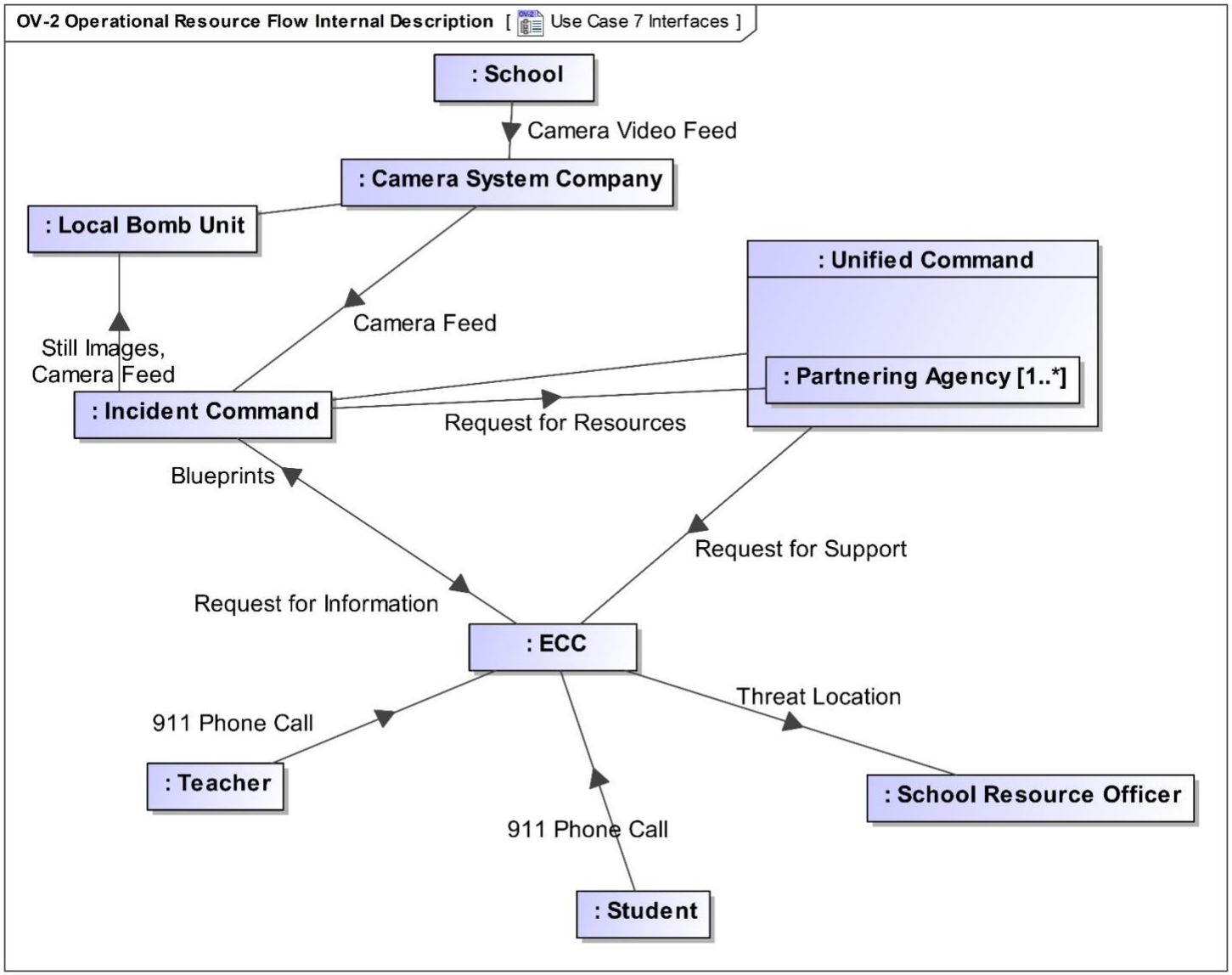
This section will be completed in the next revision.

B.5.7.4 Timeline, Information Flow, and Required Technology Capabilities

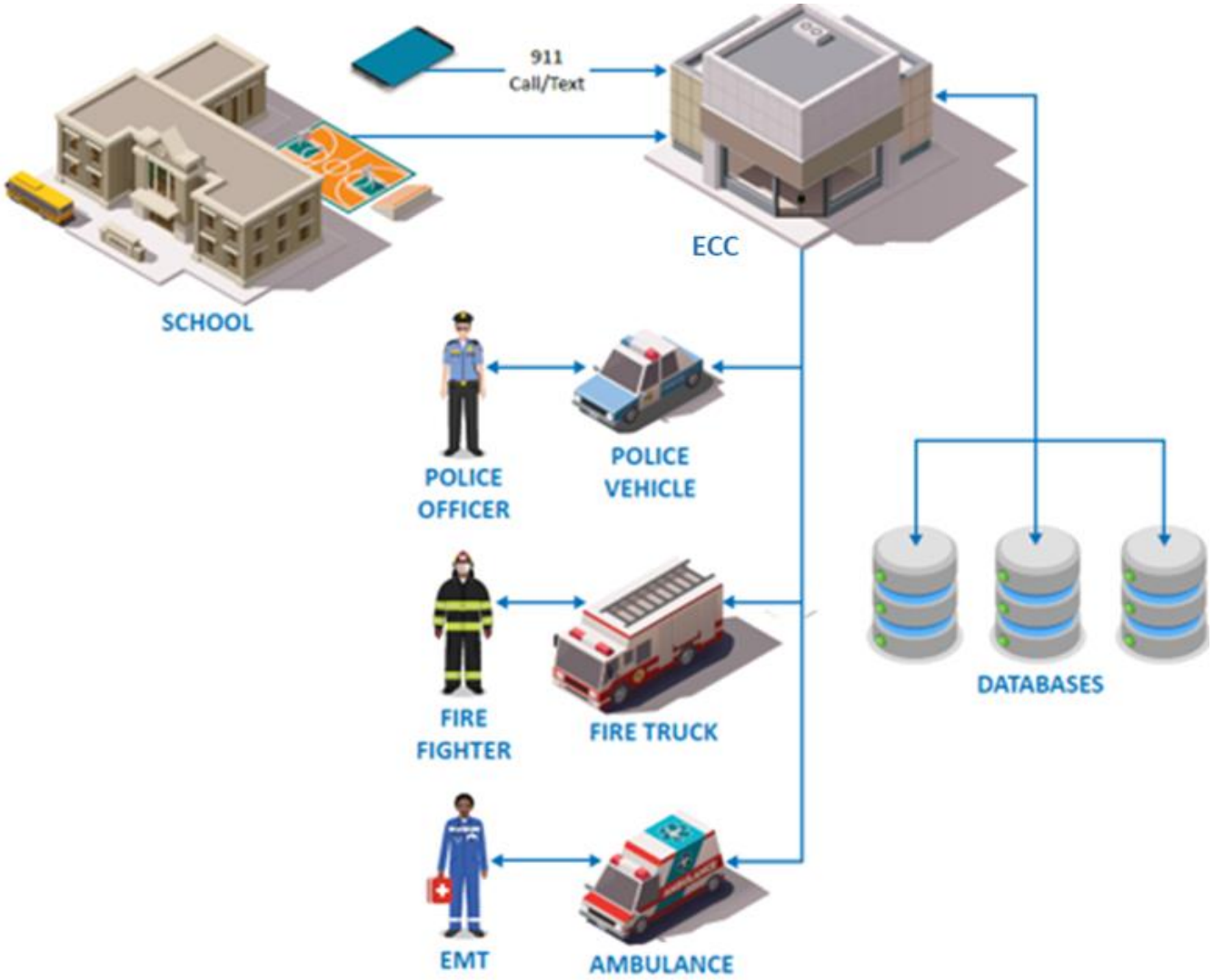
Apx Table B-13: Use Case #7: Timeline versus Stakeholders, Mission, Content, and Transport

Step	Description	Stakeholder	Mission	Content	Transport
1	A shooter enters a public school through an unsecured delivery entrance. The School Resource Officer (SRO) is in the parking lot checking parking passes. As the shooter moves through the hallways, he encounters teachers and students and fires several rounds injuring multiple people. Several nearby teachers contact the office using the in-classroom telephone reporting they hear sound of gunshots. Teachers and students call 911. The shooter continues through the school.	• Witnesses (Teachers & students) • SRO • ECC • School Office • Suspect (Shooter)	Notify the SRO (nearest onsite help) and gather intel about the developing situation.	• Voice/Audio • Video • Text-based • GPS	• School Intercom System • LTE
2	The ECC communicates with the SRO via LMR, advising the SRO of the location of the shooter so they can enter the school from a safe location. ECC personnel continue to receive multiple calls and have initiated the active shooter response protocol, and notifications are sent to police, fire, and EMS. From the incoming calls the ECC is able to relay the location of the shooter to the SRO.	• ECC • SRO • Police • Fire • EMS • Suspect	Mitigate the threat and protect the community involved.	• Voice/Audio • Video • Text-based • Alerts to Police, Fire, EMS • GPS	• LMR • LTE • Satellite (GPS)
3	Live streaming video from citizens and documents. Due to expected injuries seen on the videos, hospitals are alerted.	• Witnesses • Local Hospitals • Suspect	Analyze the severity of injuries and prepare hospitals.	• Video • Text-based • Alerts to hospitals	• LTE
4	Incident command contacts ECC and request most recent blueprints for the school.	• Incident Command • Dispatch • School Record Owners	Locate the suspect.	• Voice/Audio • Text-based • Building plans	• LTE • Radio • Wi-Fi
5	School's surveillance camera system was recently updated so real-time video is being received by the company managing the system. Video streams from school cameras are provided to incident command who uses this information to advise responding units of the shooter's location. One of the video feeds detected a suspicious device in cafeteria hallway. Photos and video are provided to	• Camera System Owners • Local Bomb Unit • Police • Suspect	Utilize onsite video to identify suspect, track movement, identify injuries, and disseminate information to responders.	• Video • Text-based (Alerts) • GPS • Images	• LTE • Radio • Mobile Data Terminals (MDTs) • Satellite (GPS) • Wi-Fi

	the local bomb unit for situational awareness and risk assessment.	• Incident Command			
6	Mutual aid from surrounding jurisdictions requested. Unified command established and real-time video displayed and tracking the shooter as he moves through the school. An electronic blue print of the school is also projected for the IC.	• Allied (Law Enforcement Mutual Aid) agencies • Suspect • Unified Command	Develop overall situational awareness and provide updates to responders.	• Video • Text-based • GPS • Building plans	• LTE • Satellite (GPS)
7	Analytical mapping capabilities are used to compare the location of the shooter via real-time video feeds with the electronic blueprint so the location of the shooter is known, as well as the locations of the injured victims. Incident Command contacts the ECC and requests UAS support for streaming live video to monitor school exits in the event the shooter flees the building. UAS video is displayed for the unified command personnel.	• Dispatch, • Unified Command • Suspect	Identify exact location of suspect and survey school perimeter.	• Video • GPS • Building plans	• Radio • LTE • Satellite (GPS)
8	State EOC activated to monitor the situation, lean forward and be ready to send additional resources. Task Force Responders (TFR) from a neighbor county are communicating with command staff and told which parking lot entrance to use as they enter the school property. The TFR lead is provided a tablet with video feeds showing the injured and locations in the school. The TFR lead executes an application that retrieves data from electronic blueprints and to help determine the exact location of the victims and the shooter within the school. TRF team is wearing body worn cameras, physiological sensors and geolocation devices and have safely entered the school and begin extracting injured victims.	• Task Force Responders (TFR) • State EOC • Unified Command • Victims • Suspect	Enable responders to safely extract victims	• Sensor data • Video	• Bluetooth • Wi-Fi • LTE



Apx Figure B-19: Use Case #7, Active Shooter – Information Flow



Apx Figure B-20: Use Case #7, Active Shooter

Apx Table B-14: Use Case #7: Required Technical Capabilities – Active Shooter

ISF Layer	Function	Capability
Data & Integration	Discovery & Data Exchange	• Third party video surveillance system • Physiological sensors - responders' health & safety • UAS live streaming video • Third party video surveillance systems • Body Worn Cameras
Integration	Transport	• Incident command provides coordination to first responders • The school alarm system is connected to the ECC • NG911 service supports calls, text, and multimedia data from the incident scene • Video from school surveillance system streamed to the ECC • Video from UAS is streamed to Incident Command • Incident command centers provide coordination
Integration	Identity Management	• Access to third party traffic cameras • Access to information about school, blueprints, local area, etc.
Integration	Analytics	• Decision support for rapid access, assessment, and dissemination of relevant data • Sensor analytics to alert IC of changes in the on-scene responders' health and location
Presentation	Monitor	• Real-time monitoring of video and biometric data • Real-time monitoring of video from surveillance system • Incident command makes informed decisions due to enhanced situational awareness

B.5.8 Use Case #8: Extreme Weather

B.5.8.1 Description

Use Case #8 describes the response to an extreme weather event. The NPSTC use case specifies a tornado, but a hurricane or earthquake could be substituted. Critical elements include loss of communications and power delivery infrastructure. In addition, first responders need to coordinate with neighboring local, state, and federal agencies.

The use case begins prior to the onset of extreme weather as atmospheric conditions become indicative of extreme weather conditions. The public safety infrastructure provides connectivity between emergency management agencies, the National Weather Service (NWS), and local weather forecasting services. As conditions indicative of a tornado begin to develop, the NWS issue warnings that are broadcast and received via smart phones. In the case of a hurricane warning, local authorities would begin to pre-position resources, including water and medicine, and depending on the severity of the storm, might begin evacuation procedures.

As tornados form and touch down, observers begin calling and texting call centers with the volume of calls exceeding the ability of individual ECCs to respond. The public safety communications architecture automatically routes the calls to ECCs with available capacity. Reports of damage to dwellings and other buildings are received and response teams are dispatched.

As soon as weather conditions ease, airborne assets – manned and unmanned – are deployed to survey the damage. Video is reviewed at command centers and incident command locations, as responders execute search and rescue activities. In addition, as people emerge from where they were sheltering, they begin to identify neighbors in need of help. Local ECCs are flooded with calls; the need for emergency medical support exceeds local resources, and incident command contacts the ECC to request mutual aid.

As EMS and firefighters from neighboring jurisdictions arrive, they work side by side with local first responders. Although their communications systems were purchased from different vendors, they support seamless push to talk voice communications with local first responders and their applications, including passing information about their location and identity to other responders.

Because of the storm, power lines and cell towers have been damaged, leaving significant areas without communications or power. First responders set up deployable ad hoc communications networks in areas where recovery efforts are hindered by the lack of communications.

B.5.8.2 Storyboard

The graphics for this section will be completed in the next revision.

Apx Figure B-21: Use Case #8, Extreme Weather – Storyboard [Figure place holder]

B.5.8.3 CONOPS

This section will be completed in the next revision.

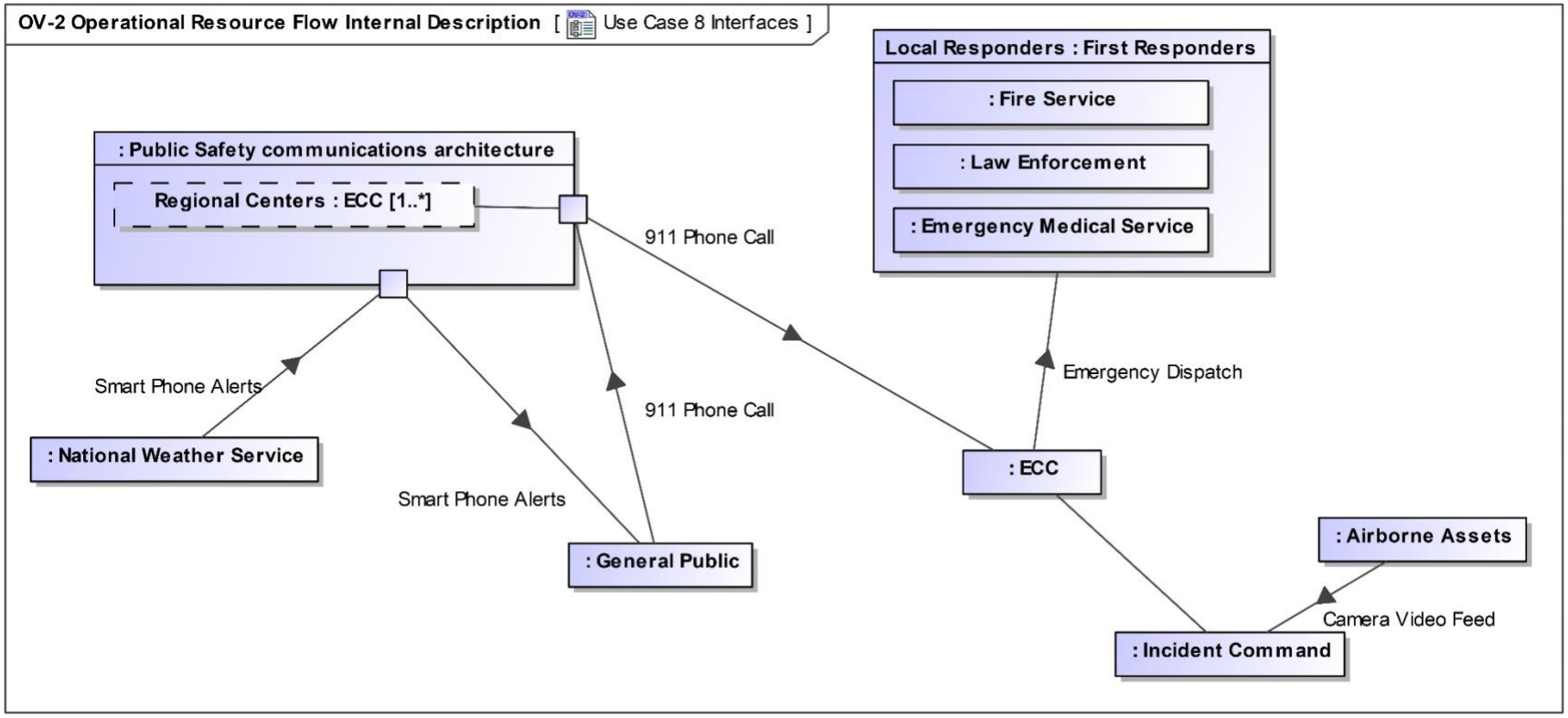
B.5.8.4 Timeline, Information Flow, and Required Technology Capabilities

Apx Table B-15: Use Case #8: Timeline versus Stakeholders, Mission, Content, and Transport

Step	Description	Stakeholder	Mission	Content	Transport
1	Atmospheric conditions become indicative of extreme weather conditions. The public safety infrastructure provides connectivity between emergency management agencies, the National Weather Service	• NWS • Emergency Management Agencies	Early detection of extreme weather conditions and	• GPS • Images • Video	• Satellite • LTE

	(NWS) and local weather forecasting services. As conditions indicative of a tornado begin to develop, the NWS issue warnings that are broadcast and received via smart phones. In the case of a hurricane warning, local authorities would begin to pre-position resources, including water and medicine, and depending on the severity of the storm, might begin evacuation procedures.	• Local Weather Services • Civilians • First Responders	prepare necessary resources.	• Sensor data	• Emergency Alert System
2	As tornados form and touch down, observers begin calling and texting call centers with the volume of calls exceeding the ability of individual ECCs to respond. The public safety communications architecture automatically routes the calls to ECCs with available capacity. Reports of damage to dwellings and other buildings are received and response teams are dispatched.	• Witnesses • ECC • First Responders	Load balance ECC calls, obtain relevant information, assess damage, and dispatch resources accordingly.	• Voice/Audio • Video • Images • Text-base	• LTE • Landlines • Radio
3	As soon as weather conditions ease, airborne assets – manned and unmanned – are deployed to survey the damage. Video is reviewed at command centers and incident command locations, as responders execute search and rescue activities.	• Airborne Assets	Assess the damage to appropriately allocate resources.	• Video	• Satellite • LTE
4	As people emerge from where they were sheltering, they begin to identify neighbors in need of help. Local ECCs are flooded with calls; the need for emergency medical support exceeds local resources, and incident command contacts the ECC to request mutual aid.	• Civilians • ECC • Volunteer Organizations Active in Disasters	Dispatch medical services as needed.	• Voice/Audio • Video • Images • Text-based	• LTE • Landline • Radio
5	As EMS and firefighters from neighboring jurisdictions arrive, they work side by side with local first responders. Although their communications systems were purchased from different vendors, they support seamless push to talk voice communications with local first responders and their applications, including passing information about their location and identity to other responders.	• Local First Responders • Neighboring Jurisdiction First Responders • Volunteer Organizations Active in Disasters	Coordinate among first responders to optimize efforts.	• Voice/Audio	• Radio

6	Because of the storm, power lines and cell towers have been damaged, leaving significant areas without communications or power. First responders set up deployable ad hoc communications networks in areas where recovery efforts are hindered by the lack of communications.	• Local First Responders • Neighboring Jurisdiction First Responders • Wireless Providers	Enable communications for first responders.	• Text-based (Alerts)	• Satellite • LTE • RF



Apx Figure B-22: Use Case #8, Extreme Weather – Information Flow

Apx Table B-16: Use Case #8: Required Technical Capabilities – Extreme Weather Event

ISF Layer	Function	Capability
Data & Integration	Discover & Data Exchange	• Infrastructure sensors provide information regarding the state of infrastructure, including power and water • Aerial sensors, helicopters, and UASs, provide SA • Physiological sensors - responders' health & safety • UAS live streaming video • Body Worn Cameras
Integration	Transport	• Incident command provides coordination to first responders • NG911 service supports calls, text and multimedia data from the incident scene • Video from victims and witness streamed to ECCs, social media, etc. • Video from UAS is streamed to Incident Command • Ad hoc networking enables emergency communications despite damage to communications and power infrastructure
Integration	Identity Management	• Access to third party camera systems • Access to infrastructure information • Access to social media reporting
Integration	Analytics	• Decision support for rapid access, assessment, and dissemination of relevant data • Sensor analytics to alert IC of changes in the on-scene responders' health and location
Presentation	Monitor	• Monitoring of infrastructure sensors, video, cellular, etc. keeps EOC's informed and able to lean forward to prepare for resource coordination (local, state, and federal staffed • Real-time monitoring of video and biometric data • Real-time monitoring of video from surveillance system • Incident command makes informed decisions due to enhanced situational awareness

B.6 Common Functional Capabilities

The following functional categories provide an overview of the core baseline capabilities identified through the Use Cases. These capabilities include the five Integration Layer functions 1) discovery, 2) identity management, 3) data exchange, 4) transport, and 5) analytics as well as the monitor function of the presentation layer.

B.6.1 Discovery and Data Exchange

The public safety community will require enhanced access to sensor data. They must be able to discover that data quickly and be able to rapidly exchange the data needed.

- Wearable sensors – The combination of wearable sensors, personal area networks, and enhanced device interoperability will enable increased situational awareness of first responder status, including improved assessment of conditions of stress or danger.
- Aerial data – Data, especially video and images, from aerial platforms (UASs) will continue to be a critical component of public safety situational awareness.
- Robots – In addition to UASs, other types of robots will eventually be employed to perform reconnaissance and provide early warning of threats to first responders.
- Third party video – Video from private surveillance systems, public utilities, and transportation departments can greatly enhance first responder situational awareness; control of cameras would increase their ability to support the public safety mission.
- Smart grid sensors – Smart grid sensors and controls can be leveraged to provide enhanced situational awareness and early detection of threats.

B.6.2 Transport

The public safety community will require increasingly robust capabilities to transport (send and receive data):

- From air to ground – The public safety community will require reliable transmission from air assets to ground command centers.
- Robust reliable 911 services – Public safety requires a robust capability to enable the public to provide information in the form of voice, text, or other multimedia data. This capability supports not only the initiation of incident response, but is a critical source of information to first responders.
- Mission Critical Push To Talk (MCPTT) – Voice communications is the primary communications asset demanded by the public safety community. MCPTT is a suite of voice related capabilities, including the ability to set up and manage groups and floor control, at the heart of public safety communications. Robust, reliable MCPTT between first responders responding to an incident or with incident commanders or ECCs, remains a vital component of public safety communications. The need for reliable MCPTT extends to the ability to interoperate with first responders from other jurisdictions.
- Connectivity with all response partners – Continuity of communications with all local, state, and federal partners from all disciplines.
- Connectivity with public – The public safety community needs the ability to provide information regarding on-going activities with the public.

B.7 Monitor

The public safety community will require the ability to monitor on-going rescue efforts through the presentation of information.

- First Responder Status – Public safety will require increased awareness of the status of first responders and the ability to detect threats and health and safety risks. Integration with biometric and other sensors will enable early detection of health or stress issues, toxic conditions, and perhaps the presence of weapons.

- Resource Status – Public safety agencies require capabilities to monitor the location and availability of their resources, including both first responders and equipment.
- Infrastructure Status – 5G enabled networks and sensors will provide enhanced situational awareness regarding the condition of infrastructure, enabling first responders to avoid threats.

B.8 Identity Management

The public safety community will require secure access to a range of data.

- Governmental Data – Public safety agencies and first responders require secure, need-to-know based access to governmental data, including driving records, criminal records, and outstanding warrants. Access will be required across jurisdictions and levels of authority.
- Third Party Data – Public safety responses will be informed by data from third party sources, including video surveillance systems, smart building sensor and control systems, and non-public databases. Gaining access to much of this data is more than a technology problem, it also requires developing policies to determine when data can be accessed, how it can be used, and how it will be protected. Examples of potentially useful but protected data include the following:
    - Privately owned (and potentially more current) building plans
    - Lists of staff and students at a school
    - Information about the residents living in a building where an incident response is underway
- Medical Data – This data is protected and governed by the Health Insurance Portability and Accountable Act (HIPAA) privacy rules that fall under the U.S. legislation for data privacy and security to safeguard information. Efforts related to medical data will need to be addressed via Health and Human Services (HHS).

B.9 Analytics

The public safety community will require the ability to process and analyze data to ensure valid and useful information is provided (e.g., right information at the right time to the right location):

- Geographical Information Systems (GIS) – GIS provides critical situational awareness, enabling the public safety community to track people and resources and understand the environment during incident response.
- Video Analytics – Video analytic capabilities enable the public safety community to consume video data. The time required to consume data makes monitoring of large amounts of video impossible. Increased use of video analytics is critical to making effective use of video.
- Data Curation – Curation services enable public safety to understand data as it is transformed into information to support decision-making. As the ability to acquire, move, and store data increases, there is an increased need for curation of that data as well as the need for decision-support tools.

B.10 BIBLIOGRAPHY

- AOS-18-0484 "First Responder Communications Data Sharing Assignment: Public Safety Communications Evolution from Voice to Data – Legacy, "As is" and "To Be" Architectures", JHU APL 27 May 18.
- "Turning Data into Information: Information Sharing Framework Task Force (ISFTF) Initial Framework Discussion Meeting" DHS CISA and APL Presentation to ISFTF on 12 August 2019.
- National Public Safety Telecommunications Council (NPSTC), "Public Safety Internet of Things Use Cases Covering Multiple Disciplines. Draft March 2019.
- Worldwide Incident Command Services Corp. (2016). Next-Generation Incident Command Best Practices Fire and Rescue Operations User Guide. Accessed 14 February 2018 and available at dhs.gov/sites/default/files/publications/NICS-Best-Practices-Fire-Rescue-508_0.pdf
- Contestabile J. (2011). Concepts on information sharing and interoperability. Domestic Preparedness, 23 March 2011. Accessed 15 February 2018 and available at: domesticpreparedness.com/preparedness/concepts-on-information-sharing-and-interoperability/
- DHS OEC. (2017). Emergency Services Sector Profile. US Department of Homeland Security (DHS) Office of Emergency Communications (OEC). Accessed 15 February 2018 and available at: dhs.gov/publication/emergency-services-sector
- SAFECOM (2018). SAFECOM: Assuring a safer America through effective public safety communications. Cybersecurity and Infrastructure Security Agency. Accessed 21 March 2018 and available at: cisa.gov/safecom/resources#
- VQiPS. (2013). Digital Video Quality Handbook. Security Industry Association - Digital Video Subcommittee and the Video Quality in Public Safety (VQiPS) Working Group. Accessed 14 February 2018 and available at: dhs.gov/sites/default/files/publications/Digital%20Video%20Quality%20Handbook.pdf
- Project 25 Technology Interest Group. (2016). Technology Benefits of P25. Accessed 14 February 2018 and available at project25.org/index.php/news-events/334-new-whitepaper-technology-benefits-of-p25
- Pew Research Center. (2018). Mobile Fact Sheet. The Pew Charitable Trusts, 2018. Accessed 3 April 2018 and available at: pewinternet.org/fact-sheet/mobile/
- NASNA. (2018). NG911 & FirstNet Together Building the Future of Public Safety Communications. National Association of State 911 Administrators (NASNA). Accessed 21 March 2018 and available at: 911.gov/pdf/NASNA_National_911_Program_NG911_FirstNet_Guide_State_Local_Authorities.pdf
- ICTAP (2009). P25 Features Matrix: User List. US Department of Homeland Security Office of Emergency Communications Interoperable Communications Technical Assistance Program. Accessed 22 March 2018 and available at: project25.org/images/stories/ptig/docs/P25%20Features%20Matrix%20Combined.pdf
- NPTSC. (2018). Public Safety Land Mobile Radio (LMR) Interoperability with LTE Mission Critical Push to Talk. National Public Safety Telecommunications Council (NPTSC). Final Report January 8, 2018. Available at: npstc.org/download.jsp?tableId=37&column=217&id=4031&file=NPSTC_Public_Safety_LMR_LTE_IO_Report_20180108.pdf
- Kaste, Martin (2018). Years After Sept. 11, Critical Incidents Still Overload Emergency Radios. National Public Radio All Things Considered. 12 March 2018. Accessed 22 March 2018 and available

at: npr.org/2018/03/12/591906701/18-years-after-sept-11-critical-incidents-still-overload-emergency-radios

- DHS S&T (2016). Datacasting: Houston Datacasting Integration Pilot After Action Report, HSHQPM-15-X-00122, July 2016. Prepared for The First Responders Group Office for Interoperability and Compatibility by The Johns Hopkins Applied Physics Laboratory. Available at: dhs.gov/publication/datacasting-houston-integration-pilot-aar
- Gibbs, C. (2017). Verizon to take on AT&T with dedicated network for first responders. FierceWireless, 16 August 2017. Available at: fiercewireless.com/wireless/verizon-to-take-firstnet-dedicated-network-for-first-responders
- PSAC. (2014). Use Cases for Interfaces, Applications and Capabilities for the Nationwide Public Safety Broadband Network, 21 July 2014. Public Safety Advisor Committee (PSAC).

Appendix C POLICY CONSIDERATIONS

Appendix C was developed for all public safety personnel with decision making roles and responsibilities and is based on the recognition that when implementing the Information Sharing Framework (ISF) there are factors beyond technologies that need to be considered. Policy considerations are part of these key factors. As an exemplar, a policy framework was developed by the Video Quality in Public Safety (VQiPS) Policy Subcommittee in an effort to capture policy considerations for entities looking to collect and utilize closed circuit television (CCTV) video. This policy framework can be genericized and utilized for other public safety data policy considerations. The goal of the policy framework is not to provide a specific policy or process solution. User needs and the ways in which data can be utilized vary significantly between users, therefore, policies should be flexible in order to accommodate these varying needs. This policy framework presents users with a set of considerations for the preparation of written policies and offers some approaches to meeting policy challenges that other jurisdictions have utilized. Users must make policy decisions based on a complex matrix of use requirements, resource availability, and the constraints of local laws and regulations. However, while the resulting policy may vary from jurisdiction to jurisdiction, the process of developing an effective policy should address certain overarching issues.

C.1 OVERARCHING SUBSTANTIVE ISSUES

A policy framework requires consideration of the following five overarching substantive issues: 1) clearly articulated public safety goals, 2) understanding and accommodation of privacy concerns, 3) attention to the security of networks and data, 4) transparency in the conduct of data collection, storage, and use, and 5) common issues in the operation of public safety programs, including technology considerations, interoperability, and continuity of operation. These issues have been summarized in the following sections.

C.1.1 PUBLIC SAFETY GOALS

A written policy statement outlining public safety purposes and goals is an important step in demonstrating the public safety purpose or purposes that government seeks to accomplish. However, such policy statements are only the beginning of the process to assure the public of the government's acceptable use of this information. Written policies need to be developed to ensure the integrity of the systems and that their use is only for a legitimate government purpose. Audit programs must be developed and implemented to ensure appropriate use in practice. Where misuse is identified, it must be met with properly documented corrective action, including the discipline of individuals involved in misuse. Programs require strict compliance with written policy to ensure use is consistent with legitimate governmental interests.

C.1.2 PRIVACY ISSUES

As a general rule, under both federal and state law, there is no cognizable protection against observing and recording conduct occurring in a public space. However, protection of privacy in public has been afforded in some circumstances, such as conversations in public places, where the individual can demonstrate a reasonable expectation of privacy in the conduct [10]. Additionally, there are clear concerns where enhanced technology is used in a public space to observe private property [11]. Thus, where a system is developed to observe public conduct, it needs to be limited in scope to public areas and cover only visual imagery and not audio voice recordings.

In addition to questions of what kinds of activity and conduct can be observed or recorded on public safety systems, the development of complex computer systems that can interrelate large amounts of public surveillance data poses additional potential issues. While the U.S. Supreme Court has not extended Constitutional protections of public data, review of some of those decisions demonstrate concern over potential privacy impacts of publicly collected data. Accordingly, careful consideration needs to be given to management of the data collected.

Whether or not a privacy impact statement is required, users seeking to implement a public safety system would benefit by considering the following essential elements in the design and operation of a system. Any written policy should explicitly discuss:

- Why the data is being collected and retained?
- Whether sensors will be covert (hidden) or overt?
- Whether there will be notice given to those in the area (i.e., with signs)?
- How the data will be used?
- What analytics (i.e., automated systematic computational analysis), if any, will be applied to the data?
- Whether attempts to identify individuals in the data will be made systematically or on a case-by-case basis?
- What other information will be combined with the data as part of processing?
- Who is authorized to view the processed data?
- How long the data will be retained under normal circumstances?
- What measures will be necessary to block or override automated deletion?
- Whether the results of analytics are stored directly with the data or stored elsewhere?
- Whether additional privileges are required to access the results of data analytics?
- What procedures will be followed in order to disclose the data to others, both inside and outside the organization?
- What procedures will be followed prior to public disclosure of data?

C.1.3 Security Issues

As with privacy, security considerations should be addressed in all aspects of creating and managing public safety systems, as well as any systems that interact with the greater public safety data ecosystem. Security is critical to ensuring the availability of the system and the integrity of its data. Inadequate security of the system will leave users unable to access critical data or to rely on the accuracy of collected data. Moreover, a lack of proper security impairs the ability of government users to ensure that data is only utilized for proper governmental purposes and that the privacy of individuals is protected.

The provision of security must address both logical and physical realms [18]. The provision of security requires an understanding of vulnerability to physical and virtual attack from both external and internal sources. For example, the U.S. Department of Defense provides guidance for designing electronic security systems, including protecting CCTV video data [19]. In every process for system operation, thought must be given to protecting components and data from compromise and improper use. As systems grow more complex and networks grow larger, that challenge increases. The rapidly growing range of hardware and software utilized for system operation further enhances the challenge. The tasks of access control and system security are essential elements implicating a range of virtual and physical security measures. Those measures should be identified in written policies.

Communications between the sensors and storage systems should be encrypted to prevent eavesdropping and hacking. If the sensor is remotely controllable, the controls should be secured to prevent unauthorized access — for example, with a complex password or with Public Key Infrastructure (PKI) certification. It may also be appropriate to use encryption to protect data at rest, either using an encrypted storage container or an encrypted video format. Encryption may also be appropriate for data that is exported to removable storage devices. Sensors that communicate wirelessly or over the public Internet are further susceptible to jamming through wireless interference or denial-of-service attacks.

Systems that provide for monitoring, analysis, analytics, and storage should similarly be secured to prevent unauthorized access. Systems that can be accessed over the Internet, such as cloud computing systems, may require additional security measures such as a physical token. Systems should have an audit trail so that staff access can be monitored. Data that is no longer needed should be securely deleted or overwritten.

C.1.4 Transparency Issues

The sensitive nature and scope of the data captured by public safety systems may cause great concern among a wide range of individuals and groups. The privacy issues outlined above give rise to substantial public attention. Even when the public goals are well documented and accepted, there is often public concern over the willingness and ability of government agencies to limit activities to stated goals and ensure matters like privacy and security of data are adequately enforced.

Transparency is both a strategic concept for policy planning and an operational concern regarding the monitoring of operations. Thus, ensuring transparency in data collection and use has two key components: commitment to system openness in the promulgation of policy, and establishment of mechanisms to ensure compliance with policy requirements. The first factor centers on the process of policy formulation and articulation. The second factor requires a strong routine of performing audits.

C.1.5 Common Technical Issues in Operations of Public Safety Systems

C.1.5.1 Technology Considerations for Data

Government agencies should develop a clear vision and scope for the purpose of the public safety system to be developed. A formal *Charter* is recommended to specify these elements, as well as the following:

- Who will be the project sponsor?
- What is the source of funding for the system?
- Who will be the customers and stakeholders of the system?
- What will be the governance structure for the construction, as well as operation of the system?
- Where will the governance structure organizationally reside?

When developing the project or portfolio of projects to develop the system, understanding the *people-oriented aspects* and *processes associated with the technology* will also be critical to ensure alignment of the technology and adoption of the system.

A plan should be developed, including a Project Approach document, which will outline all the elements to be considered when formulating a Project Implementation Plan and to refine the Project Scope. This should include the following (asterisks indicate steps requiring sponsor and stakeholder concurrence):

- Stakeholder assessment
- Functional requirements*
- Current state assessment
- High-level solution design*
- Development of implementation plan
- Development, posting, and communication of requests for proposals (RFPs)
- Conduct vendor evaluation & selection*
- Planning and procurement phase close-out & lessons learned
- Kick-off design and implementation phase of fusion project
- Project implementation and acceptance

Once the goals for the system and scope for the project have been defined, it is recommended that a team comprised of both technical and functional stakeholders use, as a benchmark, other instances where a system of similar size and scope is operational. It is important that this process not be done purely within an IT organization or team. Benchmarking against another jurisdictions will allow for better understanding of lessons learned regarding technologies and approaches. It will also aid in understanding the many variables to be considered in the system design and deployment.

The following variables need to be considered in the larger goals and scope of the system context:

- Standalone system or part of a larger network or system
- Data source locations
    - What is the geography/mission to be covered?
- Specifications for technical infrastructure
    - Size, capacity, bandwidth, speed, etc.
- Data source specifications
    - What is required for mission vs. infrastructure?
- Analog (if existing) vs. digital system
- Need to accommodate legacy or emerging technology
    - Need to scale over time vs. one time design/build/operate approach
- User locations
    - Distributed vs. centralized
- Connectivity/backhaul availability
- Retention period for recorded data
- Acceptable data quality and response time
- Active monitoring vs. recorded data and availability for incident management and response
- Number of concurrent users
- Job tasking on the same sensors
    - For example, will they be used to support more than one objective?
- Analytics and automation requirements
- Extra-system data sharing (e.g., partnerships) and interoperability
- Security (network, data center, and camera) sensitivities
- Mission criticality and acceptable outages
- Ownership of data sources (operational decisions for user priorities and access) and content
- Customization vs. ease of support
- Compliance with existing IT standards
- Ownership of technology vs. content
    - Centralized vs. distributed, strategic/core vs. necessary for operations
- Tolerances for proven vs. emerging technologies
- Mobile and nomadic needs
    - Ground, marine, and air
- Environmental considerations

When developing a public safety system and beginning the procurement process, consideration should be given to starting small and using a pilot or proof of concept that will allow for learning what will best meet the needs for the mission at hand and for determining how homogenous or variable a system design will ultimately become.

It is recommended that objective subject matter experts provide assistance with the design, selection, build, and quality assurance process. This expertise may be from one individual, a consulting firm, or a large engineering firm with integration expertise. There are positive and negative implications with any of these options, so it is important to understand what will be best in a given instance. Objectivity is most important in identifying the correct technology for the mission and in avoiding solutions that may prove limiting in the future.

It is important to have a solid description, functional requirements, and scope of work for evaluation and procurement. Depending on the products, the solutions will be some combination of hardware and software. Additionally, a criteria matrix for what is being evaluated should be developed, and a team of evaluators should provide input. Depending on the solution being considered for purchase, user demonstrations and scoring may also be part of these criteria to evaluate which best meets their requirements. Typical criteria are:

- Vendor/product references and qualifications in projects of similar size and scope
- Vendor reputation and reliability in the marketplace
- Vendor installer experience with the same product
- Cost

- Availability of local support
- Recurring costs after implementation
- Complexity to support
- Warranty
- Adherence to existing agency/company standards
- Technical solution vs. functional requirements
- User experience
- Ability to train internal resources to support

If the procurement is to be made by a governmental agency, the existence of purchasing contracts or cooperatives may be another major consideration in the selection process. If RFPs or bid processes are required, it is recommended to consider a high-technology best value approach for the procurement as opposed to a lowest-bid/winning bidder approach. The latter may not adequately take into account the proposed solution quality or vendor reputation. Best value provides for the ability to show that, while the cost may be higher, the overall return on investment (ROI) or highest value will be the best selection. This usually is evident in selection factors addressing quality, minimization of outages and down time, supportability, flexibility, ability to customize, scalability, non-proprietary in nature, lower future support costs, and so on. A facilitator may moderate the evaluation process, including administering any system demonstrations and scoring, while a procurement officer should conduct the actual vendor selection and award. This should increase alignment of the final solution to the original goals and objectives.

C.1.5.2 Interoperability for Data Sharing

Considering interoperability among system components and with other systems is very important when designing and implementing a public safety system. Although a system may be established using the best available standards and practices for the type of system being built, there may be multiple components from different vendors being used as building blocks in the overall system. When designing the system, the performance and interoperability of the entire end-to-end system should be tested, as well as when new components are used to build out the reach and capability of the system.

Each given product may have features that are proprietary and may not necessarily facilitate interoperability across system components. Making certain that different components work together is a system engineering problem and one that must be addressed by the system owner.

Public safety needs require that the quality of the data be taken into account all the way from the source to the end user. Extensibility and scalability of the vendors' products are also important because the system may be expanded over time, so obsolescence needs to be minimized to save future costs. Including interoperability in the overall system design will likely drive open-architecture or interoperability requirements in the procurement specifications to the vendor. The policy for interoperability should include considerations for connecting with and leveraging existing infrastructure, as well as emerging technologies.

Another key consideration with regard to interoperability will be the requirement to partner or share data with other jurisdictions or agencies. The data system owner should develop and approve a sound network architecture and integration approach that complies with standards and security requirements, as well as addresses other areas of concern. This model can then be repeated and validated with the various partner agencies. A stable platform of proven, open, scalable, and reliable products will facilitate the ability to develop data-sharing partnerships. The more closed or proprietary a system, the less possible this becomes (without spending more time and money on custom solutions or additional vendor products).

One approach to achieving interoperability involves having the agencies that share data purchase all of their equipment and software from the same or compatible vendors. However, because different jurisdictions often have different funding and budget schedules, policies, and processes, requiring each agency to use the same vendor technology is generally not practical unless the entire region is collectively and simultaneously upgrading their technology.

C.1.5.3 Continuity of Operations

Assuring Continuity of Operations (COOP) requires planning and coordination among agency personnel and outside vendors providing program support. Agencies should assess their risk and develop measures to prevent and control disruptions, as well as to quickly restore processes and systems after a disruptive event has occurred. When developing the agency's COOP plan, it is important to determine what functions of the public safety system are mission critical. Establishing recovery time objectives not only will set expectations for the level of service to be provided, but also serves as the basis for mapping recovery processes and capabilities. During the planning process, agencies should engage key stakeholders including partnering agencies, vendors, cloud services, etc. This will help ensure that roles, responsibilities, and capabilities are clearly defined in advance.

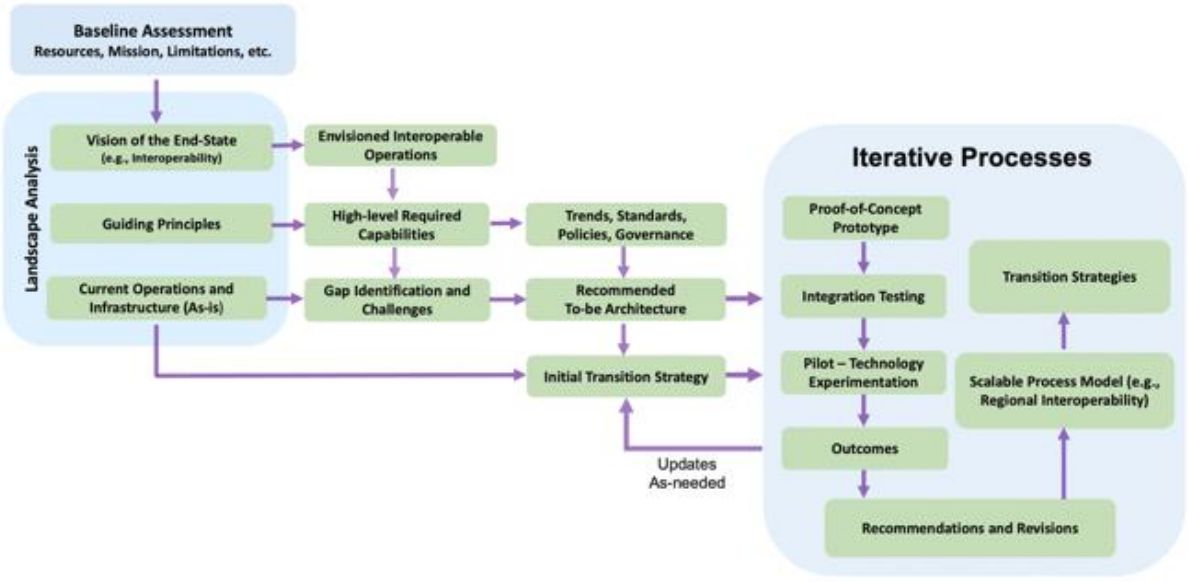
C.2 References

Department of Homeland Security Science and Technology Directorate's Video Quality in Public Safety Report; Policy Considerations for the Use of Video in Public Safety (June 2016) dhs.gov/publication/vqips-policy-considerations-use-video-public-safety

Appendix D FUNCTIONAL AND PHYSICAL ARCHITECTURE APPROACH OVERVIEW

Appendix D is intended for use by the public safety information technology (IT) community and is more technical in nature to help bridge the understanding of the interoperability needs of the end-user and the technology community.

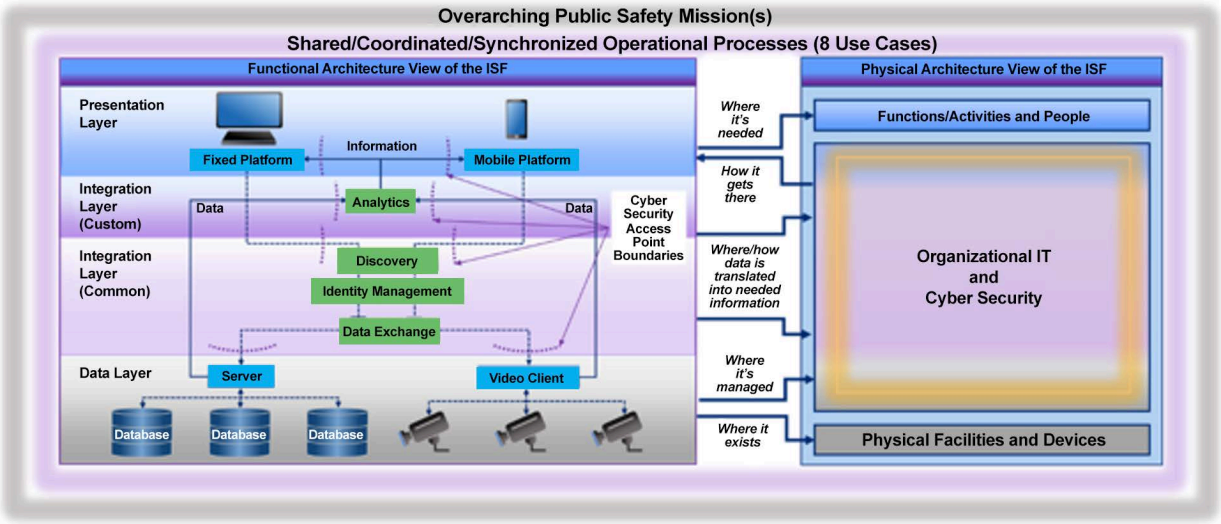
The design of an enterprise architecture, in this case for Information Sharing across Enterprises, must be initiated with a concise definition of scope, using multiple dimensions including mission, business processes and activities, organization structure, software applications and services provided, computing and storage platforms if applicable, networks and communications, and physical facilities/locations where the variety of operations takes place. A scope rubric needs to be established and utilized throughout the life of the architecture development and implementation to prevent scope creep. The National Public Safety Telecommunications Council (NPSTC) provides the End State Vision and Guiding Principles that will drive the architecture. Envisioned Operations are derived from the Vision and are documented in the IoT Use Cases. This is used to derive the High Level Required Capabilities balanced by the Guiding Principles given above. A baseline assessment of the current operational enterprise conducted during Phase 1 provides the As-is, point-in-time architecture, and the projected technology evolution (i.e. Next Generation-911, Internet of Things, 5G, etc.) provides the current trajectory for modernization. Analysis of the baseline against the defined Required Capabilities will identify potential capability gaps and inform the To-be architecture. The Required Capabilities also provide a focus for performing technology-based experimentations that can be applied to the To-be architecture. Once the To-be architecture is created and approved by the Information Sharing Framework Task Force (ISFTF), fulfillment of capability gaps from the As-is to the To-be will inform and initiate programs to achieve a managed and **interoperable ready** architecture. This disciplined process is depicted below in generic terms in Apx Figure D-1 below.



Apx Figure D-1: Developing the Framework Architecture

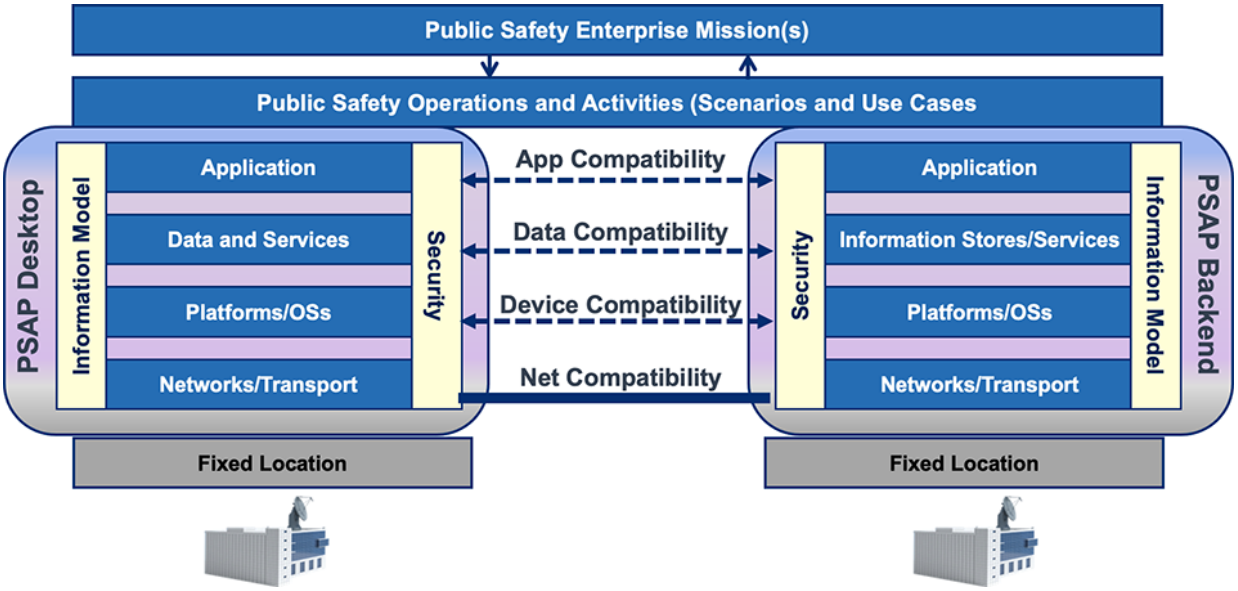
Apx Figure D-2 below illustrates the relationship between the functional and physical architectures that are the underpinning for the fundamental logical layers. Note that in this figure the overarching public safety missions (gray outline surrounding the visual) and the Operational Processes (purple outline surrounding the visual) influence much of what will comprise the functional layers. The Public Safety Missions and Operational Processes should then guide interoperability discussions and inform decisions to achieve the interoperable ready architecture and help to define the components [functional] and the infrastructure [physical] required to ensure a *complete interoperable system*. As previously noted, considerations for cyber security requirements should be

incorporated early on and be built into the interoperable architecture to ensure that information is securely transported throughout that architecture.



Apx Figure D-2: Logical Layer Translation to Functional and Physical Architectures

The transition strategy in the end may provide migration plans for any or all of the scope dimensions previously stated. Each step of this process will need to be documented in terms of the scope dimensions. *As an example,* a generic scope rubric is shown below in Apx Figure D-3 illustrating Emergency Communications Center (ECC)-to-ECC communications as a starting point for the fleshing out of the physical architecture and function components that reside within an information sharing model.



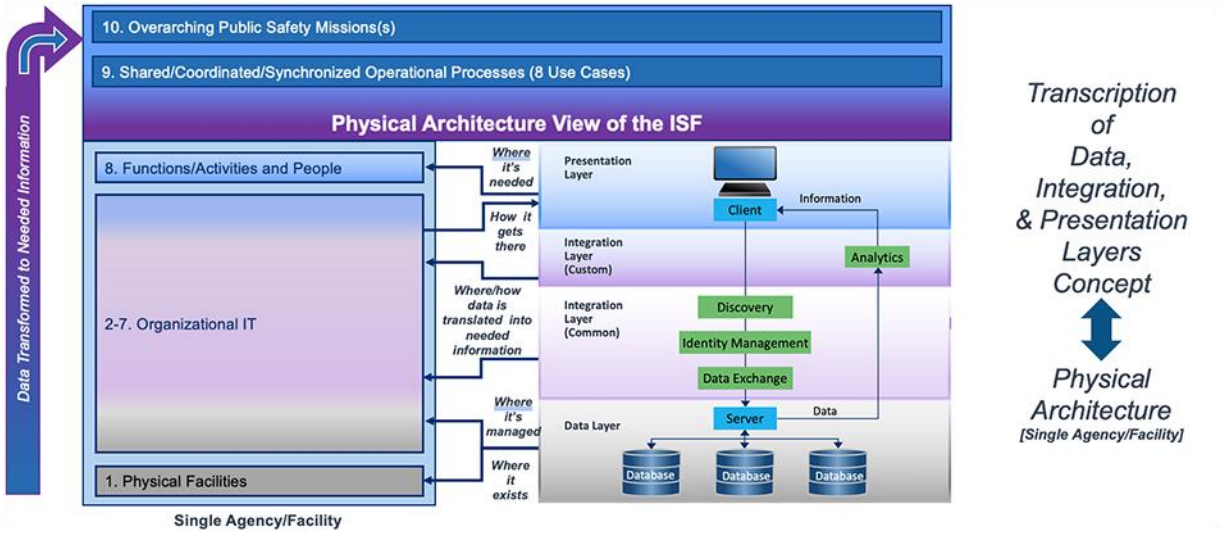
Apx Figure D-3: Initial Physical Architectural View Rubric

The top two dimensions (i.e. Mission and Operations) have been fairly well defined in previous efforts. At this point, we will further detail the second dimension by creating the functional view of the architecture, identifying all of the functional activity *entities or nodes that are involved* in all of the 8 use cases. Next, leveraging the use

cases, we will develop a set of *Enduring Functional Exchange (EFE)* categories that will drive the functional requirements for all of the physical dimensions of the interoperability interface. A diagram will be developed to show the functional nodes and the EFEs between and among them. Such a diagram should remain fairly static throughout the architecture and implementation process. Underlying technology can evolve over time that implements these EFEs, but the exchanges should remain enduring.

Examples of EFE categories are: Situation Awareness, Command and Control (Tasking), Raw Data such as from sensors, Information, and Tipping/Alerting. The characteristics of these EFEs drive the technical implementations in the physical architecture over time. For example, alerting as a functional exchange between public safety entities will always require very low latency in order to appropriately respond to the alert. Today, due to technological limitations, alerts between entities may happen via a phone call, whereas in the future (to-be architecture), the alert may occur between entity applications via sub-second pub/sub messaging mechanisms, alerting appropriate entities as needed even down to the closest emergency responder. The key is to identify and characterize the EFEs at a functional level with required implementation parameters that, over time, will drive the reference and solutions architectures as the technology and infrastructure dimensions change.

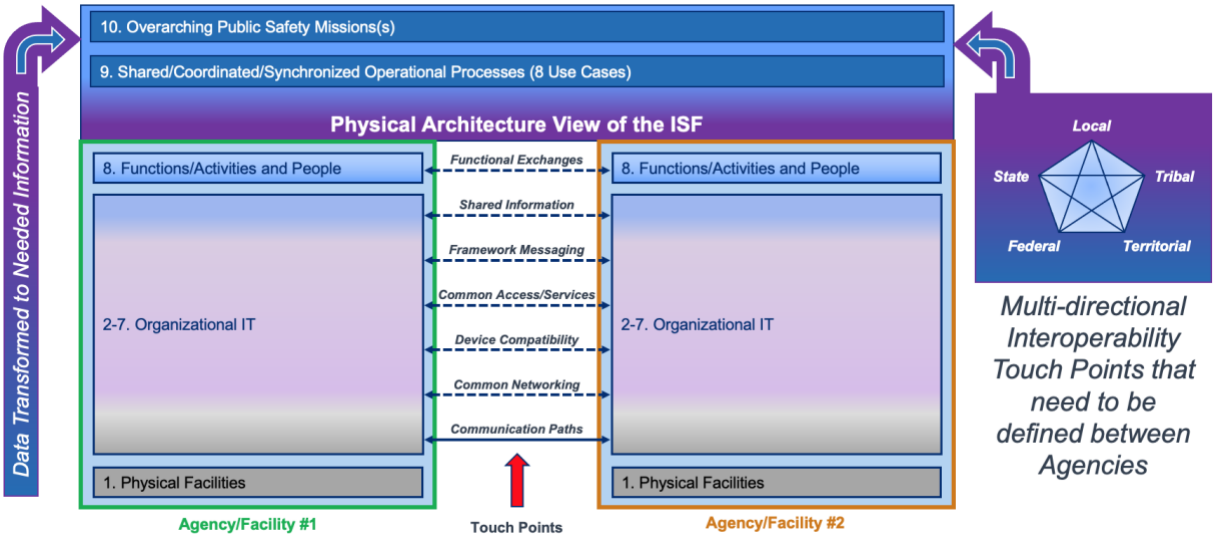
Apx Figure D-4 shows the transcription of the functional layers of the ISF to the Physical Architecture within a given agency or facility.



Apx Figure D-4: Driving Interoperability at Several Dimensions [Single Agency/Facility Interoperability Concept]

Apx Figure D-5, a more detailed decomposition of Apx Figure D-3 and Apx Figure D-4, depicts a model that has been used within other large government-based Enterprise of Enterprises information sharing architectures. A model like this is recommended for facilitating discussions among the ISFTF members to logically walk through the implications of the top-down functional architecture at the higher dimensions. Applying the EFEs to required information exchanges between and among specific entities in the Enterprise (witnesses, ECCs, Dispatch Centers, etc.), will drive solution architectures for shared information between user applications, software framework messaging, common services across the enterprise with enterprise-wide access mediation, device compatibility, common networking, and finally shared communications media such as 5G Cellular. Agency 1 and Agency 2 could represent any of the entities identified in the functional architecture and the partner entity with which they must share information via the functional exchanges. Walking down the figure, the functional exchanges will identify what types of information or data need to be exchanged between the entities and the characteristics that that exchange (e.g., latency, bandwidth, point-to-point vs. broadcast, etc.). This will then drive discussions on the best framework messaging standards to use to most efficiently exchange that information as

well as illuminating any issues with the discovery and access of that data/information and subsequent protection of that data/information if captured as part of evidence of an investigation. At this point in the process, device compatibility with these standards and access restrictions can be discussed (do we need a common device or can my device talk to your device?) as well as what networks on which these devices communicate. Information cannot be electronically exchanged if the networks are independent. Finally transport discussions that tie in the logical three-layer view architecture will illuminate any transport issues associated with all of the above interfaces.



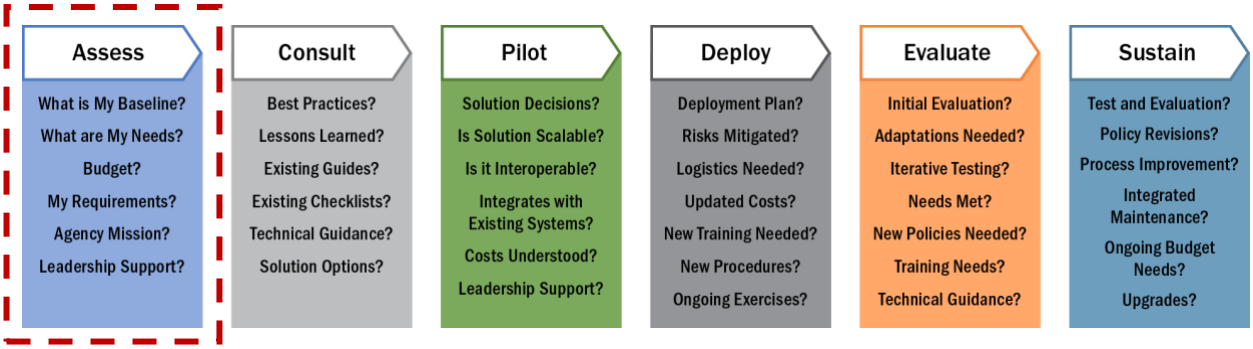
Apx Figure D-5: Driving Interoperability at Several Dimensions [Multiple Agencies/Facilities Interoperability Concept]

Appendix E ISF IMPLEMENTATION CYCLE

Appendix E provides examples and delineates how each of the six (6) steps of the Information Sharing Framework (ISF) Implementation Cycle *could be used by public safety personnel who have responsibilities for implementing interoperability programs (e.g., acquisition, training,Concept of Operations (CONOPS) development, etc.)* Steps are highlighted within the ISF Implementation Cycle and are provided below along with questions, tools, and resources that can act as guides for how to successfully complete each step and move on to the next. It is envisioned that Appendix E would transition to a suite of tools made available to public safety end-users and that training and technical support would be provided for implementation.

Note about references: The Cybersecurity and Infrastructure Security Agency (CISA) has developed reference guides, fact sheets, case studies, templates, and other documents to aid the emergency response and national security and emergency preparedness community in establishing emergency communications capabilities. Many direct references to these documenets are provided in this section. The reader should consult the following to ensure they are accessing the most recent versions. EMERGENCY COMMUNICATIONS GUIDANCE DOCUMENTS AND PUBLICATIONS

Assess



Purpose

The **Assess** step in the ISF Implementation Cycle first requires that the mission owner perform a thorough internal assessment of their missions' needs. Understanding an agency's missions is key to identifying the data content and transport mechanisms required in the Integration Layer of the ISF Framework. Other important activities in the Assess step include identifying the level of support and resources from your agency's management to include a project team of internal stakeholders, and a process to identify the appropriate missions and CONOPS. Without such support, the implementation of the ISF will be challenging, if not impossible.

Questions to Ask Yourself

- What are my **missions**?
- Have I developed an envisioned CONOPS?
- Have I identified my **stakeholders**?
- What **content** do I regularly access?
- Is there **content** that would be desirable to access but is not currently accessible?
- What communication and **transport** paths are available?
- Do I understand the available communications systems (**transport**)?
- Do I have a sufficient budget or will I need to implement my ISF in phases?
- Is agency management supportive?

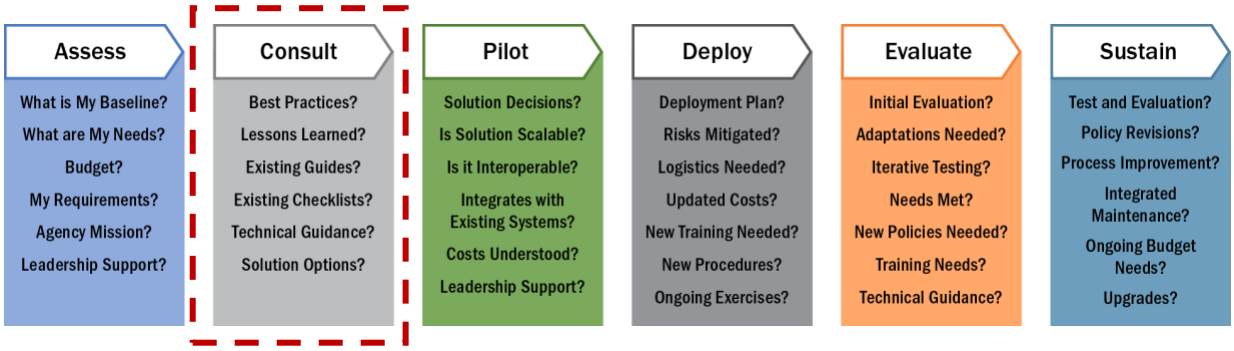
Tools and Resources

- ISF Mission Owner/Content Owner Questions (Section 4.6)
- ISF Decision Tree (Section 4.8)
- NPSTC Use Cases (Appendix A)
- National Emergency Communications Plan (NECP) Assessment Guide
- Next Generation 911 Self-Assessment Tool
- NECP Resources

Checklist for Transition to Consult

- ☐ Build a project team of internal stakeholders and secure management support for the effort
- ☐ Identify the missions, break each down into a sequence of steps
- ☐ For each missions' steps, identify the stakeholders, data content, and transport
- ☐ Walk through the ISF Decision Tree to identify the components of your Integration Layer
- ☐ Consolidate, and prioritize if needed, components identified across all missions

Consult



Purpose

The **Consult** step in the ISF Implementation Cycle requires that the mission owner perform a thorough collaborative evaluation of their missions with external partnering stakeholders. Understanding the external stakeholders' involvement in the mission(s) is important to validating the previous internal assessment. In addition, during the consult step each mission owner should identify what their partnering stakeholders have done regarding data sharing and new technology initiatives. It is important to leverage these existing initiatives to inform the building of the five functions of the integration layer. Other important activities include conducting external surveys, identifying lessons learned, and seeking technical guidance. It is important to consult external stakeholders in order to achieve maximum interoperability and to identify and address any policy barriers particularly between agencies.

Questions to Ask Yourself

- Have I consulted with my external stakeholders to understand both our needs?
- Are there regional efforts at achieving interoperability that can be leveraged?
- What lessons have my peer agencies learned?
- Are there checklists or handbooks to guide me? Have you used the ISF Decision Tree?
- Do my peer agencies have templates for writing policies and procedures that I can leverage?
- Can I get some technical expertise to support me to help me understand and document my requirements?

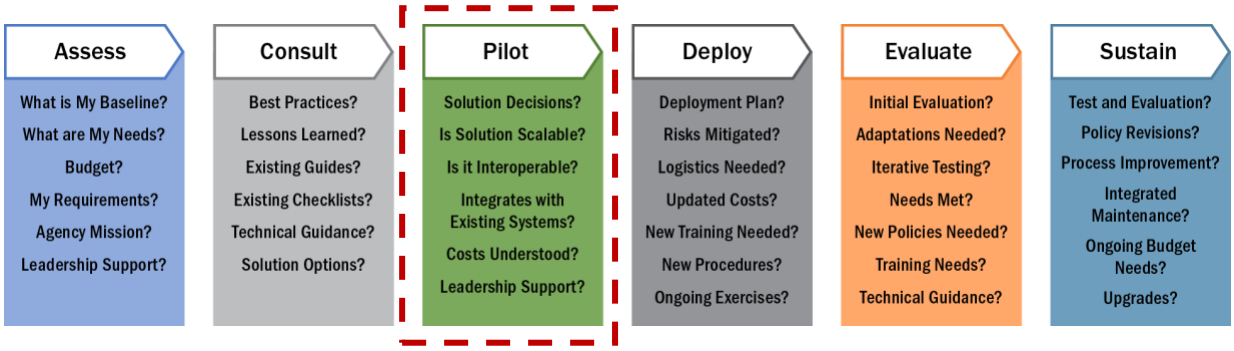
Tools and Resources

- Technical Assistance Program
- Technical Assistance Program Fact Sheet
- Interoperable Communications Plan Template
- Creating a Charter for a Multi-Agency Communications Interoperability Committee
- Lessons Learned from RapidCom
- SAFECOM Recommended Guidelines for Statewide Public Safety Communications Governance Structure
- Writing Guide for a Memorandum of Understanding (MOU)

Checklist for Transition to Pilot

- ☐ Secure regional support for the effort
- ☐ Document an understanding of how other regional agencies are approaching information sharing
- ☐ Develop list of systems requirements (derived from mission analysis, lessons learned, and consultation with stakeholders' both external and internal IT)
- ☐ Develop draft of IT systems architecture
- ☐ Develop procurement documents and procure systems for implementation

Pilot



Purpose

The **Pilot** step in the ISF Implementation Cycle requires that the selected solution be prototyped and tested among the stakeholders to validate requirements and determine how well it supports the missions. The pilot should first be configured and tested in a development environment. It should then be tested in a field environment that mimics the operational environment as closely as possible. It is also important that the system "-ilities" (scalability, reliability, availability) and security of the system be exercised. The pilot also serves as a mechanism to establish and test system interfaces before being operationally deployed. Based on the performance of the pilot, cost projections should be developed that will provide insight into the costs associated with a full deployment (including hardware, software, training, licensing, maintenance, etc.). Additionally, any policies and procedures necessary to support deployment should be developed and field tested prior to full deployment.

Questions to Ask Yourself

- Have I defined the components required in each of the 3 layers of the information sharing **framework**?
- Is there a test environment and test plan to evaluate solutions?
- Have I developed the necessary **policies** and **processes** to support the technology?
- How can I evaluate success of the effort?
- Have I addressed **security**?
- Have I addressed Identity, Credential, and Access Management (ICAM) procedures within my agency and with partnering agencies?

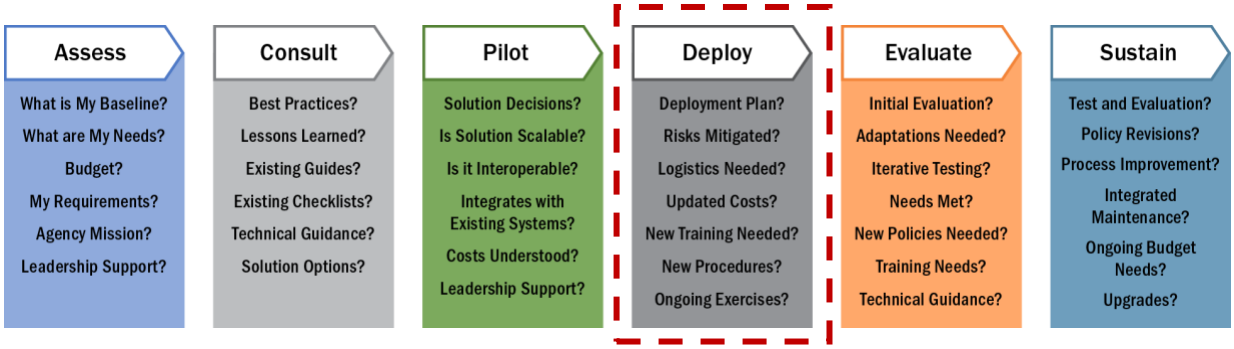
Tools and Resources

- Technical Assistance Program
- CISA ICAM Resources

Checklist Transition to Deploy

- ☐ Receive procurement approval
- ☐ Document Test Plan and execute
- ☐ Document the deployed systems architecture
- ☐ Develop System Security Plan (SSP)
- ☐ Develop policies and procedures to support operation
- ☐ Partnering stakeholders have credentials for utilizing ICAM protected data and information
- ☐ Develop cost projections for operational deployment

Deploy



Purpose

The **Deploy** step in the ISF Implementation Cycle requires the fielding of the system within the selected organizational entity (single agency, multi-agency, etc.). The project team should first develop a deployment plan that aligns with operational and budgetary constraints. As the team works to implement the plan they should be conducting hands on training with end users. The successful deployment of the system requires that risks have been identified and corresponding mitigation steps have been developed. Lastly, cost estimates should be revisited to ensure that projections align with the actual costs.

Questions to Ask Yourself

- Have I developed a deployment plan? Is it phased?
- What risks do I have and how to I mitigate them?
- Have I updated my costs for implementation?
- Have I implemented the necessary training to use the system?
- Do I need to have a coordinated tabletop, limited field test, etc. for all system users?
- Will the ISF capabilities and functionalities be incorporated into the day-to-day routine so that using the system will become second nature to system users?

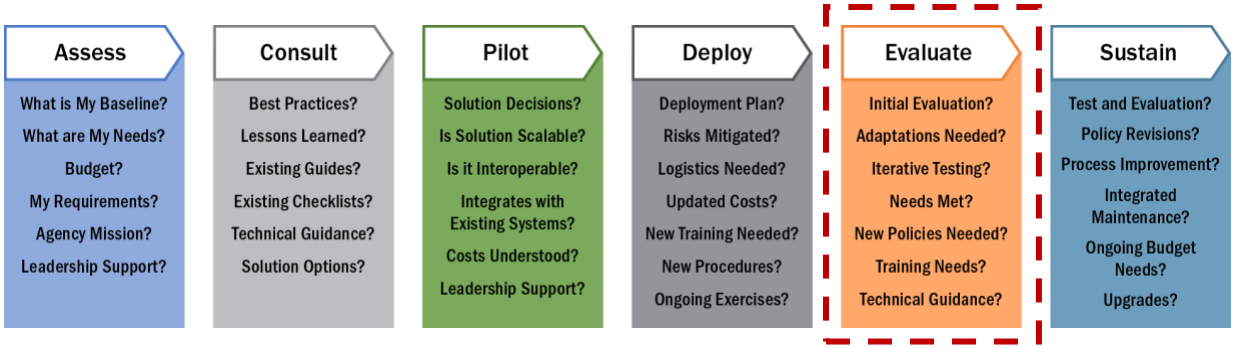
Tools and Resources

- National Interoperability Field Operations Guide

Checklist for Transition to Evaluate

- ☐ Create Deployment Plan
- ☐ Receive Authority to Operate and deploy the system
- ☐ Develop Risk Assessment and Mitigation Plan

Evaluate



Purpose

The **Evaluate** step in the ISF Implementation Cycle requires that the deployed system be assessed and measured to ensure that it meets each mission's needs and requirements. The project team should develop a plan that outlines the mechanisms in which they will collect system metrics and the frequency in which they will be collected. The metrics should confirm that each mission's needs are being met. The project team should also assess whether revisions are needed to policies, procedures, or training efforts. Efforts should be made to set up the necessary governance structure to ensure management buy-in and continued success during sustainment.

Questions to Ask Yourself

- Have I monitored and assessed the deployment to determine revisions to technologies are warranted?
- Have I coordinated with **stakeholders** and users to ensure that each mission's needs are met?
- Have I set up the necessary **governance** and oversight procedures?
- Have I set up a process to capture metrics? At the appropriate intervals?
- Have I identified the appropriated trainees?
- Have I documented the necessary training **procedures** and user manuals?
- Is there sufficient technical guidance for ongoing **technology** maintenance?
- Are there processes in place to quickly address unexpected issues encountered when using the system?

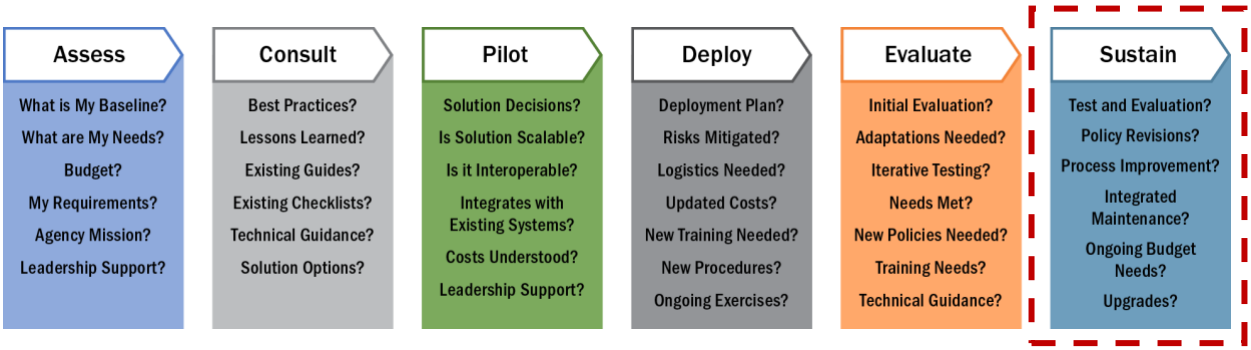
Tools and Resources

- Establishing Governance
- Governance for Officials
- Performance Measurement Guide
- Homeland Security Exercise and Evaluation Program

Checklist for Transition to Sustain

- ☐ Develop Plan to Capture and Document Metrics
- ☐ Updated Training Materials and Technical Guidance
- ☐ Governance Procedures have been established
- ☐ Confirm all missions' needs have been met with stakeholders and users

Sustain



Purpose

The **Sustain** step in the ISF Implementation Cycle requires the support necessary to maintain the production system over time as well as identify any change in conditions which would require system revisions. This includes all the support elements for *people, process, and technology* success such as funding for maintenance, training, and technology support, and governance processes to resolve user needs to ensure the continued operation of the system. Going forward a process is required to identify new stakeholder requirements and the corresponding system improvements.

Questions to Ask Yourself

- Does my sustainment plan include funding for maintenance and upgrades?
- Is there a schedule for exercises to identify new technologies that would better meet mission needs and to maintain user proficiency?
- Does the CONOP need to be revised?
- Are revisions to policies and procedures needed?
- Is the **governance** structure suitable for long term sustainment?

Tools and Resources

- SAFECOM Sustaining Public Safety Resources
- SAFECOM Public Safety Funding Resources

Do You Need to Go Back and Assess?

- As user experience and exercises identify new user requirements, you should consider going back through the cycle.
- The scope of the new requirements will determine if the current system can be modified or requires new users, policies, and/or technology approach.

Appendix F Acronym Lists

F.1 Document Acronym List

Acronym	Definition
AC	Access Class
ACB	Access Class Barring
AI	Artificial Intelligence
AMBE	Advanced Multi-Band Excitation
AMR	Automatic Meter Reading
APCO	Association of Public-Safety Communications Officials
API	Application Programming Interface
APL	Johns Hopkins Applied Physics Laboratory
APN	Access Point Name
ARP	Allocation and Retention Priority
CAD	Computer Aided Dispatch
CCTV	Closed Circuit Television
CISA	Cybersecurity and Infrastructure Security Agency
COML	Communication Unit Leader
CONOP	Concept of Operation
COOP	Continuity of Operation
CSfC	Commercial Solutions for Classified
CSSI	Console Subsystem Interface
D-D	Device-to-Device
DFSI	Digital Fixed Station Interface
DHS	Department of Homeland Security
DHS PIV	Department of Homeland Security Personal Identity Verification
DoD CAC	Department of Defense Common Access Card
DOT	Department of Transportation
ECC	Emergency Communications Center
ECD	Emergency Communications Division

ED	Emergency Department
EDXL	Emergency Data Exchange Language
EFE	Enduring Functional Exchange
EMS	Emergency Management System
eNodeB	E-UTRAN Node B
EOC	Emergency Operations Center
EoE	Enterprise of Enterprises
EPC	Evolved Packet Core
ESInets	Emergency Service Internet Protocol Networks
FEMA	Federal Emergency Management Agency
FICAM	Federal ICAM
FirstNet	First Responder Network Authority
GBR	Guaranteed Bit Rate
GCSE	Group Communications System Enablers
GIS	Geographic Information System
GPS	Global Positioning System
HAZMAT	Hazardous Materials
HHS	Health and Human Services
HID	Human Interface Device
HIPAA	Health Insurance Portability and Accountable Act
HPA	High Priority Access
HTTP	Hypertext Transfer Protocol
IC	Incident Command
ICAM	Identity, Credential, and Access Management
IMS	Incident Management System
IoT	Internet of Things
IP	Internet Protocol
ISF	Information Sharing Framework
ISFTF	Information Sharing Framework Task Force

ISSI	Inter Radio Frequency (RF) Subsystem Interface
IT	Information Technology
ITSL	IT Service Unit Leaders
IWF	Inter-Working Function
JSON	JavaScript Object Notation
LMR	Land Mobile Radio
LTE	Long Term Evolution
LTE-D	LTD Direct
MCF	Media Cohesion Framework
MC-PPT	Mission Critical Push-to-Talk
MDT	Mobile Data Terminal
ML	Machine Learning
MO	Mobile Originating
MT	Mobile Terminating
NASTD	National Association of State Telecommunications Directors
NCS	National Communications System
NCSWIC	National Council of Statewide Interoperability Coordinators
NECP	National Emergency Communications Plan
NFC	Near Field Communications
NG911	Next Generation 911
NGBR	Non-Guaranteed Bit Rate
NGFR	Next Generation First Responder
NIMS	National Incident Management System
NLP	Natural Language Processing
NPSBN	National Public Safety Broadband Network
NPSTC	National Public Safety Telecommunications Council
NS/EP	National Security/Emergency Preparedness
OAUTH	Open Authorization
OCC	Operation Control Center

OMA	Open Mobile Alliance
OTT-PTT	Over-the-top Push-to-Talk
P25	Project 25
PDN	Packet Data Network
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PoC	Push-to-Talk over Cellular
ProSe	Proximity Services
PS IoT	Public Safety Internet of Things
PSTN	Public Switched Telephone Network
PTSA	Public Safety Technology Alliance
PTT	Push-to-Talk
QCI	Quality of Service Class Identifier
QoS	Quality of Service
RAN	Radio Access Network
REST	Representative State Transfer
RF	Radio Frequency
RFP	Request for Proposal
RFSS	Radio Frequency Sub-System
RMF	Risk Management Framework
RMS	Record Management Systems
ROI	Return of Investment
RoIP	Radio over Internet Protocol
RRC	Ration Resource Control
RSA	Rivest-Shamir-Adleman
RTCC	Real Time Crime Center
SAFECOM	CISA managed organization, not an acronym
S&T	Science and Technology
SCIP	Statewide Communication Interoperability Plan

SCP	Secure Copy Protocol
SOAP	Simple Object Access Protocol
SOP	Standard Operating Procedures
SRO	School Resource Officer
SSL	Secure Socket Layer
SSO	Single Sign On
SWIC	Statewide Interoperability Coordinator
T-3	Triage, Treatment, and Transport
TFR	Task Force Responders
TIA	Telecommunications Industry Association
TOC	Traffic Operation Center
UAS	Unmanned Aircraft System
UC	Unified Command
UE	User Equipment
URL	Uniform Resource Locator
V2X	Vehicle to Everything
VoLTE	Voice over LTE
VQiPS	Video Quality in Public Safety
WB-Security	Web Services Security
WISER	Wireless Information System for Emergency Responders
WSDL	Web Service Description Language
XML	eXtensible Markup Language

F.2 Common Emergency Communications Acronym List

Acronym	Definition
ALI	Automatic Location Information
BCF	Border Control Function
CAD	Computer-Aided Dispatch
CAMA	Centralized Automatic Message Accounting
CHS	Call Handling System
DBMS	Database Management System
DMZ	Demilitarized Zone
ECC	Emergency Communications Center
ECRF	Emergency Call Routing Function
ESInet	Emergency Services Internet Protocol Network
ESN	Emergency Services Number
ESRP	Emergency Services Routing Proxy
FCC	Federal Communications Commission
FirstNet Authority	First Responder Network Authority
GIS	Geographic Information Systems
LIS	Location Information Server
LMR	Land Mobile Radio
LNG	Legacy Network Gateway
LPG	Legacy Public Safety Answering Point Gateway
LSRG	Legacy Selective Router Gateway
LTE	Long-Term Evolution
LVF	Location Verification Function
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NENA	National Emergency Number Association
NGCS	Next Generation Core Service
NG911	Next Generation 911

NIEM	National Information Exchange Model
OSE	Originating Service Environment
OSP	Originating Service Provider
POC	Person/Point of Contact
PRF	Policy Routing Function
PSAP	Public Safety Answering Point
RFIA	Request for Assistance Interface
RTP	Real-Time Transport Protocol
SICP	Statewide Interoperability Communications Plan
SIEC	Statewide Interoperability Executive Committee
SIGB	Statewide Interoperability Governing Body
SIP	Session Initiation Protocol
SMS	Short Message Service
SOP	Standard Operating Procedure
SS7	Signaling System No. 7
SWIC	Statewide Interoperability Coordinator
TDM	Time-Division Multiplexing
TFOPA	Task Force on Optimal Public Safety Answering Point Architecture