



CISA
CYBER+INFRASTRUCTURE



SAFECOM[®]

NCSWIC[®]



Emergency Communications Systems Value Analysis Guide

April 2020

EXECUTIVE SUMMARY

SAFECOM and the National Council of Statewide Interoperability Coordinators (NCSWIC), in collaboration with the Cybersecurity and Infrastructure Security Agency (CISA), released the *Emergency Communications Systems Value Analysis Guide* to assist public safety agencies evaluate communications systems and equipment for cost effectiveness and value to its users. This document describes common system components, including considerations and features required by public safety agencies that are unique to specific roles of the agency or individuals who will use the equipment. The information contained in and accompanying this document is intended to inform planning and cost estimation through the entire system lifecycle, as communications investments and sustainment should be included in every year's budget. It is not intended as an all-inclusive, comprehensive step-by-step manual; rather, a collection of considerations, guidance materials, and best practices developed by the public safety user community in SAFECOM and NCSWIC.

During a value analysis, agencies consider quantitative and qualitative metrics based on user requirements, proposed solutions, and alternative costs, benefits, and risks to determine the solution best aligned with their strategic goals. It is important to assess and identify unnecessary costs and use of resources, which do not support or maintain efficiencies, quality of service, capabilities, performance, or extend the longevity of services. Agencies should evaluate public safety requirements such as [public safety grade](#) expectations for equipment to remain operational and fully-functional in an all-hazards environment, as well as adoption of technical standards that improve interoperability across system components. In addition, agencies should consider the need for continuous investments beyond the initial capital expenses to support operating and maintenance costs, anticipated lifespan of equipment to plan for eventual replacement, and integrated operations with partner agencies during budget development.

Establishing interoperability between existing critical communications networks and evolving technologies is another way to promote efficiencies. As such, another recommendation encourages agencies to collaborate with partners across all levels of government to actively share infrastructure, equipment, and services in support of public safety communications. This approach is known as [Shared Communication Systems and Infrastructure \(SCSI\)](#), which recognizes the value of building communications networks that support multiple agencies and disciplines. SCSI benefits include improved spectrum use; optimized resource usage and management; streamlined operations; reduced capital, operations, and maintenance expenditures; and enhanced economies of scale.

The *Value Analysis Guide* provides descriptions, costs, and expected lifespan of common system components (e.g., Infrastructure, Fixed Station Equipment, Devices, Accessories, Features, Software and Data Storage) used by public safety agencies, with considerations of key features based on the specific user's position and responsibilities. These features should inform planning and cost estimation to include relative cost increases (e.g., inflation of service fees, taxes, technological advances, leasing costs), potential savings (e.g., partnerships, bulk purchasing, economies of scale), benefits (e.g., improving efficiencies, interoperability, security, user functions), and risks (e.g., quality of service, capabilities, performance or extending the longevity of services), as well as applicability by discipline.

With all budgeting decisions, cost and value can be a trade-off. This document offers recommendations and a Value Analysis Checklist to assist public safety agencies make these decisions. To start, agencies must assess requirements and proposed solutions, then identify unnecessary costs or potential savings through informed investments. The checklist tool summarizes analysis questions across common system components to help identify agencies' user requirements and missions to inform planning and budgeting decisions. Once identified, agencies should enact procedures to remove unnecessary costs and invest in right-sized solutions. The [SAFECOM and NCSWIC website](#) offers guidance resources developed by public safety officials and experts who have successfully managed communications systems across the Nation. In addition, [CISA Interoperable Communications Technical Assistance Program](#) is available to assist agencies with these actions.

Communications investments are among the most significant, substantial, and long-lasting capital expenditures that public safety agencies make. There is no simple solution for determining emergency communications systems and equipment; components require continuous investments to maintain services and replace parts. Procurement decisions require extensive assessments to identify user requirements, system components, and features that are cost effective and offer the right value. Public safety agencies must also balance financial challenges to keep pace with the rapid technological advancements in an era of competing priorities and constrained resources. With these realities in mind, it is recommended Governors, elected officials, and leaders collaborate with Statewide Interoperability Coordinators and other state-level planners to understand emergency communications capabilities and needs in their area, then incorporate that knowledge into planning and budgeting decisions.

TABLE OF CONTENTS

EXECUTIVE SUMMARY I

INTRODUCTION..... 1

CONSIDERATIONS 2

 PUBLIC SAFETY REQUIREMENTS 2

 CONTINUOUS INVESTMENTS AND SUSTAINMENT 3

 LIFESPAN 4

 INTEGRATED OPERATIONS 5

SYSTEM COMPONENTS 7

 INFRASTRUCTURE 8

 FIXED STATION EQUIPMENT..... 12

 DEVICES..... 17

 ACCESSORIES..... 21

 FEATURES 22

 SOFTWARE AND DATA STORAGE 23

RECOMMENDATIONS..... 24

CONCLUSION 25

 ABOUT SAFECOM / NCSWIC 25

APPENDIX: VALUE ANALYSIS CHECKLIST..... 26

INTRODUCTION

In a climate of heightened competition for public safety funding, leaders make difficult budgeting decisions while addressing a variety of state, local, tribal, and territorial needs beyond emergency communications. Agencies must be fully prepared to provide decision-makers with an explanation of mission critical communications costs and benefits to the community. The Cybersecurity and Infrastructure Security Agency (CISA) developed the *Emergency Communications Systems Value Analysis Guide* to assist public safety agencies evaluate communications systems and equipment for cost effectiveness and value to its users. This document describes common systems and equipment, including considerations and features required by public safety agencies and emergency responders. It is intended to inform planning and cost estimation through the entire system lifecycle—beginning with initial capital investments, through ongoing maintenance and operations, replacement parts, and finally disposition and transition to new capabilities once a system has reached its useful end-of-life.

All agencies, regardless of size or discipline—law enforcement, fire, emergency medical services, public works/utilities, and public safety answering points (PSAPs)/dispatch centers—must be prepared to serve and protect their citizens. Emergency responders require communications systems provide a basic level of operability, interoperability, and reliability with other responders, along with various features for security and accessories based on their role and operational responsibilities. Additional features and accessories drive up costs. However, not all system users need every feature or accessory, so agencies can save costs where possible. For example, ruggedized handheld radios and microphones are necessary for certain personnel exposed to extreme environmental elements, whereas other personnel may not require these added features.

A value analysis determines whether proposed communications systems and equipment are cost effective and offer the right value. Agencies consider quantitative and qualitative metrics based on an alternative's costs, benefits, and risks to determine the solution best aligned with their strategic goals. It is important to assess and identify unnecessary costs, which do not improve efficiencies, quality of service, capabilities, performance, or extend the longevity of services. Then, enact procedures to remove these unnecessary costs and stretch public safety funding to encompass all mission critical requirements.

Value Analysis Definition:

A disciplined approach to implementing cost control and reduction techniques to ensure an organization's necessary functions are fully operational for the minimum cost without diminishing quality, reliability, and performance.

CISA collaborated with SAFECOM and the National Council of Statewide Interoperability Coordinators (NCSWIC) to gather input from members and other public safety stakeholders responsible for various aspects of emergency communications. SAFECOM and NCSWIC recognized the need for a value analysis guide to inform decision-makers of communications budgeting considerations, public safety requirements and equipment features, and relative purchasing and operating costs to ultimately better serve the community.

CONSIDERATIONS

This section outlines key considerations before conducting a value analysis on emergency communications systems and equipment. Agencies should evaluate public safety requirements, need for continuous investments, anticipated lifespan of equipment, and integrated operations during budget development. These considerations include the specific role of the agency or individuals who will use the equipment. For example, microphone accessories will vary; law enforcement may invest in noise suppression features so officers will be heard despite traffic noise and sirens in the background. In contrast, fire service may invest in remote speaker microphones with exaggerated controls, so firefighters can operate in bulky gloves and find controls without looking at the device. While different disciplines have unique needs, this guidance is applicable to all agencies to inform communications investments.

Public Safety Requirements

Public safety agencies have mission critical requirements to support time-sensitive and lifesaving tasks. Infrastructure equipment, user devices, and methods of deployment must be hardened and resilient, allowing for prolonged operation in rigorous and harsh environments with a high-level of user familiarity, availability, and accessibility. Communications must be interoperable with partners, reliable in widespread areas, and secure against malicious actors. These requirements are described as **public safety grade**, a concept referring to emergency responders' expectation for systems and equipment to remain operational and fully-functional in an all-hazards environment (i.e., routine to catastrophic emergency response operations), during and immediately following all emergency response operations; including major natural or manmade disasters on a local, regional, and nationwide basis.¹

Resilient Communications Systems Operate in All-Hazards

Hurricane Michael made landfall in northwest Florida on October 10, 2018, as a Category 4 storm, causing most counties in the area to lose local communications systems, with some seeing their LMR tower sites fail as a result of high winds. Lacking communications hampered public safety response efforts, but that was not a challenge for agencies that subscribed to Florida's statewide system. "[The system] remained operational in the region during the hurricane, and only a few tower sites required significant repair afterward to return to operation," according to Matthew Matney—Chief of Public Safety for the Florida Department of Management Services. With the designed continuity and resiliency measures, including backup power, overlapping coverage, and route diversity, the statewide system sustained mission critical services across multi-discipline agencies. Following the storm, impacted tower sites were repaired in record time, and the system became completely operational within 96 hours of the hurricane landfall.

Source: [Urgent Communications](#)

While public safety grade is not a defined standard, agencies should design and finance communications systems to fulfill their jurisdiction's specific communications needs, as well as adopt **technical standards** to ensure and promote operability, interoperability, and provide protection from isolation and obsolescence. For example, experts recognize the Project 25 (P25) suite of standards for the design and manufacture of interoperable, digital two-way wireless communications products for land mobile radio (LMR) systems. Agencies should adhere to technical standards for all communications technologies (e.g., long-term evolution [LTE] for broadband/Internet Protocol [IP]-based systems, Common Alerting Protocol for alerts and warning systems) and invest in certified digital encryption for security. While technology is not the sole component of ensuring interoperable communications, it is a major facilitator of interoperability and common standards are essential in the current and future environment.

¹ [National Public Safety Telecommunications Council Report: Defining Public Safety Grade Systems and Facilities](#), May 22, 2014.

Public safety systems are typically built to a higher standard than commercial communications networks, including advanced network hardening and sustainability, route diversity, and backup capabilities. Consequently, these systems cost more than commercial networks. Functionality, not cost, should be the driving factor in communications investments. **Figure 1** summarizes stakeholder resources for additional information on public safety requirements encompassing operability, interoperability, security, and resiliency.

Figure 1. Resources to Better Understand Public Safety Requirements

Requirements	Resources
Operability	<p>LMR 101, Part I: Educating Decision Makers on LMR Technologies includes simple diagrams, terminology, history, and current usage of LMR technologies by public safety agencies</p> <p>LMR for Decision Makers, Part II: Educating Decision Makers on LMR Technology Issues provides information on emerging technologies, the impact such technologies will have on LMR systems, discussion of the LMR-to-LTE transition, and need to sustain mission critical voice</p> <p>LMR for Project Managers, Part III: A P25 Primer for Project Managers and Acquisition Managers introduces standards-based purchasing, and explains importance of P25 standard to public safety interoperability</p>
Interoperability	<p>SAFECOM Guidance on Emergency Communications Grants contains additional information on technical standards relevant to public safety communications systems (e.g., 911 networks, alerts and warnings, data information sharing, LMR, LTE/Internet Protocol-based broadband)</p> <p>Technology Guide for Communications Interoperability provides background and tools to carry out technology initiatives that make interoperability possible</p>
Security	<p>Considerations for Encryption in Public Safety Radio Systems examines why encryption may be needed during time-sensitive operations or when open communications may not be sufficient to protect information</p> <p>Determining the Need for Encryption in Public Safety Radios provides an overview of factors public safety agencies should consider before reaching a decision to encrypt their public safety radio systems</p> <p>Best Practices for Encryption in P25 Public Safety Land Mobile Radio Systems addresses standards-based encryption to enhance secure interoperability and minimize the risk of compromising sensitive information</p> <p>Developing Methods to Improve Encrypted Interoperability in Public Safety Communications highlights best practices of key management necessary to allow encrypted operability and interoperability</p>
Resiliency	<p>Resiliency Fact Sheet summarizes key elements to continuity and resiliency resources</p> <p>Public Safety Network Communications Resiliency Self-Assessment Guidebook and Public Safety Communications Resiliency: Ten Keys to Obtaining a Resilient Local Access Network establish a process to assess threats and vulnerabilities to communications networks, enabling organizations to conduct self-assessments and identify ideal mitigation solutions</p>

Continuous Investments and Sustainment

Making a *one-time* financial investment is not sufficient to effectively procure, operate, maintain, sustain, upgrade, and eventually replace public safety communications systems and equipment. Systems require a large initial capital investment, as well as ongoing funding for upgrades, repairs, replacement, and operations (e.g., fuel for generators). Agencies should communicate ongoing needs from the start and continually share long-term budget projections to educate elected officials and decision-makers on anticipated costs (e.g., ongoing, short-term, long-term) of communications systems. Communications investments and sustainment should be included in every year’s budget.

In addition to the Federal Government allocating funding for the Nationwide Public Safety Broadband Network (NPSBN), it is imperative for elected officials and decision-makers to understand the public safety community will continue to rely on LMR as a primary means of communications and integrate capabilities

for years to come.² Agencies must sustain legacy LMR systems by investing in maintenance and operations. This includes system-level support activities to ensure equipment is operating and functioning (e.g., managing software, access, outages, cyber incidents); maintenance activities to fix damage or prevent failures (e.g., repair); and user support for answering operational questions (e.g., helpdesk, radio shop). Agencies must continue to fund these services for effective system operation.

To capture considerations throughout the entire system lifecycle, CISA, SAFECOM, and NCSWIC developed the [Emergency Communications System Lifecycle Planning Guide](#).³ It is developed for agencies to use in their efforts to fund, plan, procure, implement, support, and maintain public safety communications systems, and eventually replace and dispose of system components. Each phase of the system lifecycle planning model—Pre-Planning; Project Planning; Request for Proposals and Acquisition; Implementation; Support, Maintenance, and Sustainment; End-of-Lifecycle Assessment and Replacement; and Disposition—includes best practices, considerations, and recommended checklists to assist public safety agencies embarking on system lifecycle planning.

Lifespan

Systems are comprised of a variety of interconnected components, each with their own optimal lifespan. This document identifies general lifecycle lengths of components, such as handheld devices (e.g., 2–10 years) or fixed station equipment and infrastructure (e.g., 7–25 years). Agencies should overlay their long-term budget projections to show interval replacement dates and investments required over time, so components are replaced on time or as needed to keep the system operating. While some system components need infrequent maintenance and operations, other components may require extensive repairs, reprogramming, or replacement (e.g., portable equipment) to maintain communications functionality. See the [Appendix](#) for a checklist of decision points to determine when to replace equipment, as well as considerations for system components.

Agencies should consider potential downfalls when using communications equipment beyond its useful lifespan. Over time, it may become increasingly difficult to service outdated equipment due to shortages in replacement parts or lack of personnel with requisite training. Vendors may end technical support, which may increase security vulnerabilities to entire systems. Outdated equipment may also inhibit full functionality of newer technologies due to data capabilities or other features. The cost of maintaining outdated equipment may eventually become costlier than investment in new systems or equipment.

System Repairs Following Disasters

As recently seen in the California wildfires, fires can grow from a small brush fire into an inferno that engulfs thousands of acres in a matter of hours. Public safety communications systems were impacted by 2018 wildfires, requiring extensive repairs or replacement. In addition to systems used by emergency responders, Governor Jerry Brown and the California state legislature are considering laws to standardize emergency alerts and overhaul 911 systems to improve notifications of fast-approaching wildfires or looming danger from other disasters, such as floods or earthquakes.

Gov. Brown said the wildfires will cost the state heavily. In addition to communication system improvements, officials are undertaking a broad, more ambitious prevention strategy that includes aggressively thinning out forests in rural parts of the state; increasing state funding for firefighters, training, and equipment; incorporating new methods for battling unpredictable, wind-driven fires; and working with local governments to update land use plans and building codes that discourage development in fire-prone areas or call for more safety measures.

Source: [Government Technology magazine](#)

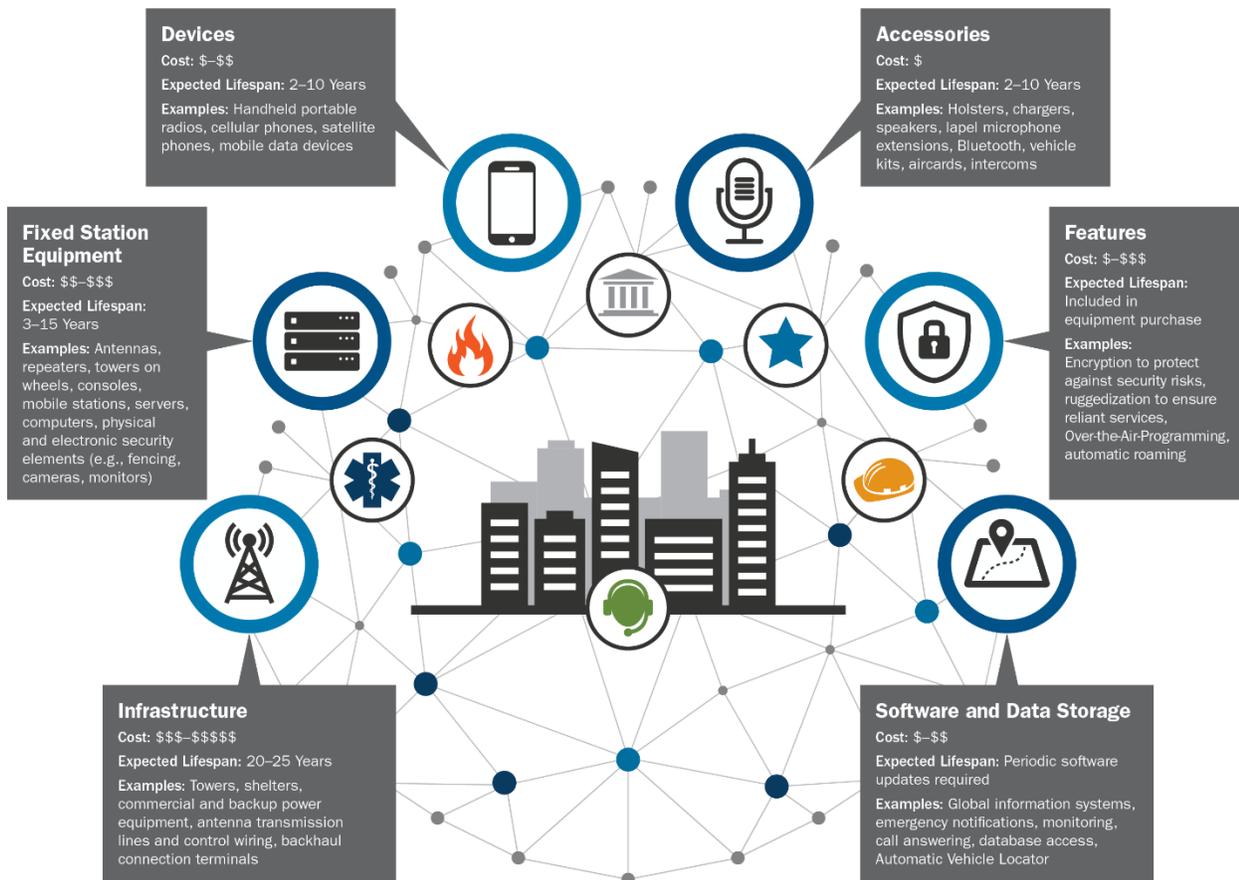
² The First Responder Network Authority's (FirstNet Authority's) mission is to deploy the NPSBN to provide LTE-based broadband services and applications to public safety entities. Currently, the network provides data and video capabilities and will later offer tactical voice communications. For more information, visit: <https://www.firstnet.gov/>.

³ [2018 Emergency Communications System Lifecycle Planning Guide Compendium](#), August 2018.

Integrated Operations

Public safety comprises multiple disciplines (e.g., law enforcement, fire, emergency medical services, public works/utilities, and PSAPs/dispatch centers) across levels of government, the private and non-profit sectors, as well as interactions with citizens. Therefore, it is strongly encouraged for agencies to coordinate communications investments across the region. **Figure 2** depicts integrated operations across multiple agencies and communications capabilities.

Figure 2. Integrated Operations Graphic



To ensure communications projects are compatible, interoperable, and support statewide plans and strategies, agencies should consult appropriate statewide leaders or entities prior to developing projects. This includes the Statewide Interoperability Coordinator and Statewide Interoperability Governing Body, which serve as focal points for interoperable communications and understand existing and planned investments across the region. Agencies should identify and share resources with public safety partners, which result in cost savings for the community.

Across the United States, many public safety agencies have recognized the value of building communications networks that support multiple agencies and disciplines through the **Shared Communication Systems and Infrastructure (SCSI)** approach. The SCSI approach pertains to the assets—physical infrastructure (e.g., tower sites, facilities, repeaters, connectivity), real estate, spectrum, applications, subscriber units, technical and operational staff—contributed in support of a reliable, resilient, connected, operable, and interoperable communications network for users. SCSI initiatives focus on encouraging active resource sharing for organizations with national security, emergency preparedness, and public safety missions. Once established, these systems can expand and grow to include other technologies, capabilities, and subscribers across all levels of government.

SCSI Benefits

- Increased operability and interoperability
- Improved spectrum use
- Optimized resource usage and management
- Streamlined intra-agency and interagency operations
- Decreased duplication of investments
- Reduced capital, operations, and maintenance expenditures
- Positive environmental impacts
- Enhanced operational coordination and economies of scale

Source: *CISA SCSI for Public Safety Communications Fact Sheet*

Strong governance is crucial to the success of any SCSI approach. As defined in the *2018 Emergency Communications Governance Guide of State, Local, Tribal and Territorial Officials*, “effective governance...facilitate[s] a greater understanding of existing communications capabilities and gaps, as well as the development of a coordinated strategic plan to prioritize resources, investments, and staffing...[resulting from] multi-disciplinary federal, state, tribal, regional, jurisdictional, and local entities working together to promote interoperability efforts.”⁴

The SCSI approach continues to gain traction. Public safety agencies are pursuing opportunities to build communications networks based on shared personnel, assets, and equipment to streamline efforts to effectively govern shared communications networks. **Figure 3** includes examples of such efforts.

Figure 3. Examples of SCSI Approach

<p>Puerto Rico (PR) and the U.S. Virgin Islands (USVI) Tactical Communications (TACCOM) Land Mobile Radio (LMR) Pilot</p> 	<p>The devastation of Hurricanes Irma and Maria created an opportunity to pursue a shared system environment in PR and the USVI. The PR/USVI TACCOM LMR Pilot will result in a robust LMR network supported by proper frequency management practices, comprehensive user education, effective site/repeater selection, and strong resiliency/security measures. This project created strong collaboration among federal participants.</p>
<p>Southwest Border Communications Working Group (SWBCWG) SCSI Project</p> 	<p>The ability to effectively communicate along the nation's Southwest Border is a known challenge. In response, the SWBCWG is working to develop a report for decisionmakers outlining the governance, policy, resource sharing, and security considerations for implementing a SCSI project in the region. Partners include federal, state, local, and tribal government and public safety organizations operating along the border.</p>
<p>Statewide Systems</p> 	<p>Many state networks already embrace SCSI tenets and have made great progress towards overcoming barriers to effective interjurisdictional and interstate communications. The SCSI approach provides them a resource for continued sharing, a path to resolve their collective challenges, and best practices for enhancing their shared systems.</p>

Multi-technology, cross-system, and cross-jurisdictional communications are essential needs for emergency responders in the 21st century. Public safety agencies can use the SCSI approach to enable: (1) effective implementation of available communications technologies and techniques; and (2) better utilization and integration of available communications assets in support of day-to-day operations and incident response. As SCSI tenets are incorporated into emergency communications governance, partners will be able to understand existing capabilities and gaps, resulting in the development of a coordinated strategic plan to prioritize resources, investments, and staffing, and promote larger-scale interoperability efforts.⁵

⁴ *Emergency Communications Governance Guide of State, Local, Tribal and Territorial Officials*, 2018.

⁵ For information on implementing the SCSI approach, visit <https://www.cisa.gov/scsi> or contact CISA at SCSI@cisa.dhs.gov.

SYSTEM COMPONENTS

This section provides descriptions, costs, and expected lifespan of common communications system components and equipment. It is not intended as an all-inclusive, comprehensive system design plan. Rather, this document includes general system components and equipment used by public safety agencies, with considerations of key features based on the specific user's position and responsibilities. These features should inform planning and cost estimation through the entire system lifecycle to include relative cost increases (e.g., inflation of service fees, taxes, technological advances), potential savings (e.g., partnerships, bulk purchasing, economies of scale), benefits (e.g., improving efficiencies, interoperability, security, user functions), and risks (e.g., quality of service, capabilities, performance or extending the longevity of services), as well as applicability by discipline. **Figure 4** summarizes common system components that are later described in subsections for Infrastructure, Fixed Station Equipment, Devices, Accessories, Features, and Software.

Figure 4. Summary of System Components, Examples, Cost, and Expected Lifespan

Components	Examples	Cost*	Expected Lifespan
Infrastructure	Towers, shelters, commercial and backup power equipment, antenna transmission lines and control wiring, backhaul connection terminals (e.g., fiber, microwave, wired)	\$\$\$-\$\$\$\$\$	20–25 years
Fixed Station Equipment	Antennas, repeaters, towers on wheels, consoles, mobile stations, servers, computers, physical and electronic security elements (e.g., fencing, cameras, monitors, environmental conditions)	\$\$-\$\$\$	3–15 years
Devices	Handheld portable radios, cellular phones, satellite phones, mobile data devices	\$\$-	2–10 years
Accessories	Holsters, chargers, speakers, lapel microphone extensions, Bluetooth, vehicle kits, aircards, intercoms	\$	2–10 years
Features	Encryption to protect against security risks, ruggedization to ensure reliant services, Over-the-Air-Programming, automatic roaming	\$\$-\$\$\$	Included in equipment purchase
Software and Data Storage	Global information system, emergency notifications, monitoring, call answering, database access, Automatic Vehicle Locator	\$\$-	Periodic software updates required

**Cost ratings are relative to each other with Infrastructure being the most expensive and Accessories being one of the least expensive system components. Costs vary depending on system configuration, owned or leased operation, geographic region, manufacturer, applicable technical standards testing, operational and maintenance costs, and other factors described in this document.*

When considering discipline-specific investments, infrastructure and fixed station equipment for public safety communications systems are generally the same regardless of size or discipline. Many states and territories operate statewide or regional systems instead of separate local communications systems. Other states and territories achieve interoperability through connections forming a “system of systems.” The goal of statewide, regional, or connected systems is to serve multiple disciplines, resulting in built-in interoperability with partners. Conversely, handheld devices, accessories, and other features may vary by discipline based on the user's role in the emergency response community. For example, 911 communicators require data and positioning systems on computers and headsets for dispatch operations, which need to interoperate with field personnel using mobile data terminals and wearable microphones ruggedized for the environment.

Infrastructure

Communications system infrastructure includes assets and connections such as towers, shelters, commercial and backup power equipment, antenna transmission lines and control wiring, and backhaul connection terminals (e.g., fiber, microwave, wired). Additional components may include console equipment, repeaters, network interconnect equipment, transmitter combiners, receiver multi-couplers, filtering equipment, base stations, antennas, microwave equipment, commercial services networks/circuit offerings, backhaul implementation equipment, and radio frequency (RF) site infrastructure. System infrastructure has an optimal lifespan of 20–25 years. Factors affecting the lifespan of the infrastructure include where the equipment is located (e.g., harsh environment) and growth or expansion of the system (e.g., need for increased shelter size, additional repeaters).

Towers



Description: Towers are arguably the most visible component of a communications system. Whether free-standing or guy-line supported, fixed towers can soar several hundred feet in the air. Alternatively, vehicular-mounted portable towers may provide additional public safety communications support during an emergency or special event.



Function: Public safety communications towers should be constructed with consideration for potential hazards (e.g., hurricanes, floods, tornadoes, forest fires), which may increase costs. Additional factors affecting the cost of towers include Federal Aviation Administration (FAA) requirements for appropriate warning lights (depending on tower height), Internal Revenue Service (IRS) tax considerations during government and industry resource sharing, site location, and meeting current environmental impact standards for the climates in which they operate. Towers should have engineering and environmental inspections to ensure they have not been overloaded with too much equipment for the wind load expected.



Usage: Users access communications towers and other infrastructure when transmitting signals.



Analysis: Public safety agencies should consider the following when installing, upgrading, or replacing towers:

- What existing infrastructure or resources can you lease or share with other organizations rather than developing new communication sites?
- What environmental impact statements (EIS) or environmental assessments (EA) are required? Will the selected site comply with the Environmental Planning and Historic Preservation (EHP) and National Environmental Policy Act (NEPA) requirements?
- Have the appropriate FAA requirements for height (i.e., above ground level), warning lights for aircraft, grounding requirements, and licensing requirements been addressed for the tower?
- Have all necessary and appropriate permissions been received before construction begins?
- Has a media and public communications plan been developed for a new radio tower site?
- Is an adequate lightning protection system in place? Are physical security and safety measures included?



Cost: Construction of a new tower is costly, generally priced in the \$\$\$–\$\$\$\$ range and often paid for over the span of multiple years. Ongoing maintenance, as well as possible leasing costs, are required in the \$–\$\$ range.



Lifespan: Towers have a lifespan of 20–25 years, possible shorter or longer depending on environmental factors.

Shelters



Description: Shelters are the physical structure to house communications equipment, power feeds, antenna transmission line and backhaul connections, and other infrastructure and fixed station equipment. Shelters are primarily permanent structures that are co-located with a tower or antenna system and built on a foundation. Equipment is frequently installed in racks and cabinets within shelters. Cabinets are smaller enclosures that house and protect communications equipment.



Function: Shelters should be purchased and installed with consideration for potential hazards (e.g., hurricanes, floods, tornadoes, forest fires, vandalism), which may increase costs. Additional factors affecting the cost of shelters include weight, size, heating, ventilation, and air conditioning (HVAC) capabilities, material composition, transportation charges, installation factors, and meeting current accessibility and power requirements.



Usage: Typically, only technical communications staff have access to shelters.



Analysis: Public safety agencies should consider the following when installing, upgrading, or replacing shelters:

- Is there adequate space for the shelter and access to the shelter?
- In the operating environment, will you encounter excess water, sand, dust, heat, or cold? What HVAC capabilities are required?
- Can the site be adequately secured from vandalism and unauthorized access? What level of access control is possible?
- Does the shelter have adequate interior space for planned equipment and room for expansion?
- Does the shelter have an adequate monitoring system for tower lighting, power systems, and environmental and security controls?
- Have specific requirements (e.g., U.S. Department of Labor Occupational Safety and Health Organization), electrical codes, industry standards (e.g., Underwriters Laboratory), and manufacturer guidance been addressed to ensure the safety, security, reliability, and operability of the communications systems?



Cost: Shelters are priced in the \$\$-\$\$\$ range as an initial capital investment and require ongoing maintenance costs in the \$-\$\$ range.



Lifespan: Shelters have a lifespan of 25 years or more depending on environmental factors.

Commercial and Backup Power Equipment



Description: Communications sites require power to operate infrastructure and equipment. Primary power is typically delivered through the commercial electric power supply system. Sites without access to commercial alternating current (AC) power utilities can use solar or wind-generated power, or a generator powered by various fuel types. Systems should have battery backups, uninterruptible power systems (UPS), or backup power generators to ensure the survivability of communications during intermittent power surges, losses of power, or extended blackouts.



Function: Backup power equipment greatly increases the resiliency and redundancy of communication functions; however, increased diversity increases costs. Multiple backup systems (e.g., generators, batteries, hydrogen fuel cells) provide reliable redundancy at differing costs. On a lifecycle basis, fuel cells can offer significant cost savings over both battery-generator systems and battery-only systems when shorter runtime capabilities are sufficient. For long-term backup power solutions, generators may be a more appropriate solution. Additional factors affecting the cost of backup power systems include the size and type of generator (e.g., gasoline, diesel, propane, natural gas, alternator, gas turbine powered), and runtime capabilities based on battery life or fuel capacity.



Usage: System designers plan for primary and backup power supplies to support mission critical operations.



Analysis: Public safety agencies should consider the following when installing, upgrading, or enhancing power equipment:

- Is commercial power available or economically accessible?
- Is commercial and backup power suitably sized for all users?
- Is there sufficient space for backup power generation in or outside the shelter?
- What is the impact if the communications site was not operating due to a power loss?
- Are both short- and long-term backup power sources needed?
- Are adequate fuel supplies accessible?
- Are start testing and load testing regularly scheduled and accomplished?
- Are your power systems monitored and alarmed?



Cost: Batteries are priced in the \$–\$\$ range and generators and their associated fuel storage containers are priced in the \$–\$\$\$ range. Ongoing maintenance costs are required to perform regular testing and resupply of fuels.



Lifespan: Batteries performance and lifespan vary depending on the operating environment. Generators and their associated fuel storage containers have a lifespan of 25 years or more.

Transmission and Wired Lines



Description: Communications systems require a multitude of transmission and wired lines to connect equipment together. Transmission lines are often coaxial cable, although many microwave communications systems use waveguide cable to send and receive RF signals to the antenna systems on towers. Wired lines may include power circuits, tower lighting conductors, video cables, telecommunications connections, and alarm and control cables.



Function: Transmission and wired lines located at sites should be installed with consideration for potential hazards (e.g., earthquakes, hurricanes, floods, tornadoes, wildfires), which may increase costs. Additional factors affecting cost include the type of line (e.g., waveguide, coaxial, fiber), protection and security of transmission lines and cable runs (e.g., anti-climb gates, underground runs, conduit encasement, tower encasement), route diversity, and redundancy.



Usage: Proper installation and maintenance of RF transmission lines and data cabling is essential to ensure an appropriate level of operability, reliability, and readiness of the system.



Analysis: Public safety agencies should consider the following when installing or replacing transmission and wired lines:

- In the operating environment, will lines encounter excess water, sand, dust, heat, or cold? Is an ice bridge required to protect lines or cables installed above ground?
- Can routing over more than one physical path be accomplished to provide route diversity?
- Will connections to other backbone networks be practical from the site?
- Are protective and restorative measures available if services are lost or congested (e.g., [Continuity Planning Suite](#), [Telecommunications Services Priority \[TSP\]](#))?



Cost: Transmission and wired lines are priced in the \$–\$\$ range as an initial capital investment, depending whether owned or leased.



Lifespan: Transmission and wired lines have a lifespan of 20–25 years with proper maintenance.

Fixed Station Equipment

Communications system fixed station equipment includes physical assets and connections such as antennas, repeaters, towers on wheels, console equipment, mobile stations that connect to infrastructure and support system operations, and physical and electronic security elements that protect these items. Additional fixed station equipment includes network interconnect equipment, transmitter combiners, receiver multi-couplers, filtering equipment, base stations, microwave equipment, commercial services networks/circuit offerings, backhaul implementation equipment, and monitoring equipment. Fixed station equipment has an optimal lifespan between 3–15 years. Additional factors affecting the lifespan of the equipment include where the equipment is located (e.g., harsh environment) and the actual operational usage of the equipment (e.g., 24/7).

Antennas



Description: Antennas and supporting equipment enable the transmission and reception of radio messages. Omnidirectional antennas are designed to provide good overall coverage whereas directional antennas provide focused coverage in a particular direction. Antenna installations require spectrum management and communications system expertise coupled with a thorough understanding of the antenna location, radio frequency power, radio system frequency, and the specific manufacturer of the antenna system.



Function: Antennas located at communications sites should be installed with consideration for potential hazards (e.g., wind, ice, flooding), which increases costs. Additional factors affecting the cost of antennas include the type (e.g., microwave), power into the antenna, and the operational use of the equipment.



Usage: Following proper antenna installation guidelines is essential to successful radio operations, as well as to limit access to areas close to the antennas.



Analysis: Public safety agencies should consider the following when installing or replacing antennas:

- In the operating environment, are additional structural supports required?
- Was an impact analysis performed when adding a new antenna to a tower?
- Was the antenna properly grounded to protect from lightning?
- Are Federal Communication Commission (FCC) guidelines followed for safe operation?
- Are antenna systems adequately documented?



Cost: Antennas are priced in the \$\$–\$\$\$ range as an initial capital investment and require ongoing maintenance costs in the \$–\$\$ range.



Lifespan: Antennas typically have a lifespan of 11–15 years.

Repeaters and Towers on Wheels



Description: Repeaters and towers on wheels are used to increase the range of handheld portable radios, mobile radios, and base stations by retransmitting received signals. Repeaters are typically installed with a well-situated antenna on a tower, building, or hilltop. From this vantage point, a repeater receives transmissions on one frequency and retransmits them on another. Portable repeaters and towers on wheels are temporarily deployed to extend a network's coverage area in planned or emergency operations (e.g., wildfire occurring outside of normal system range).



Function: Public safety grade portable and fixed repeaters and towers on wheels should be digital or analog capable, operate in assigned spectrum frequencies or be configured for cross-band operations, support conventional or trunked systems, and be compatible with technical standards-based communications systems (e.g., P25 for LMR, LTE for broadband/IP-based technologies). Repeaters and towers on wheels should also be able to pass encryption transparently.



Usage: Repeaters and towers on wheels extend the effective range of a lesser powered radio, allowing other users of the channel to hear and talk with others at greater distances.



Analysis: Public safety agencies should consider the following when installing repeaters and towers on wheels:

- Do repeaters and towers on wheels have the capability for remote management?
- Will repeaters and towers on wheels need to transmit encrypted signals?
- If temporary deployment is required where coverage is intermittent or unavailable, does the equipment offer a low power configuration, portability, and ruggedization?



Cost: Repeaters and towers on wheels are priced in the \$\$–\$\$\$ range as an initial capital investment and require ongoing maintenance costs in the \$–\$\$ range.



Lifespan: Repeaters and towers on wheels typically have a lifespan of 11–15 years.

Console Equipment



Description: Console equipment allows radio dispatchers to manage the flow of information and organize public safety agency resources. These consoles may include a telephone, alarms, messaging, voice radio, mobile data, logging systems, geographic display of call source, responder location, and street closure indications, and the ability to feed incident information to an agency's records management system.



Function: Consoles are typically hardwired to the radio system. However, in mobile command posts, the radio system link could be over the air. Additional network connections can be wireless. To achieve network route diversity, at least two unique paths must exist between the console and the base station(s)/repeater sites whether provided through leased circuits or an IP network. Console equipment can support conventional or trunked systems, operate across multiple spectrum frequencies, and be compatible with technical standards-based systems (e.g., P25 for LMR, LTE for broadband/IP-based technologies).



Usage: Dispatch operators use consoles to coordinate public safety agency operations where needed. For example, the operator can coordinate multiple responders through voice and messaging communications allowing the responders to communicate with the console operator and each other. Additionally, console dispatcher can answer Enhanced 911 and Next Generation 911 calls where available, as well as place and answer administrative phone calls.



Analysis: Public safety agencies should consider the following for console equipment:

- What type of system technologies will the console equipment service (e.g., 911, LMR, Voice over IP, LTE)?
- What is the planned usage (e.g., 24/7 dispatch, backup or temporary)?
- What programs and software will need to be integrated (e.g., records database)?
- Do communications need to be secured/encrypted?
- Is there a need to manage operations from a remote location or provide backup operations for another dispatch location?
- Can dispatch requirements be consolidated across multiple jurisdictions?
- Does your agency require audio recording capabilities?



Cost: Consoles are priced in the \$\$–\$\$\$ range as an initial capital investment and require ongoing maintenance costs in the \$–\$\$ range.



Lifespan: Consoles typically have a lifespan of 3–15 years.

Mobile Repeaters



Description: Mobile (or transportable) repeaters are radios that include all user equipment and software needed for communications within a specific network, including vehicular-mounted radio units that boost portable handheld radios.



Function: Mobile repeaters provide intercommunication to other devices on the system, as well as the fixed infrastructure depending on configuration, including between mobile repeaters and participating land, maritime, or air-based stations engaged in coordinated public safety operations.



Usage: Users communicate with other users on the system using mobile repeaters, similar to handheld portable radio units. For example, utility mobile repeaters can be installed in vehicles that provide maintenance, fire and crash protection, freight handling, or other group support normally under control tower direction at an airport. Mobile repeaters may also connect with airborne platforms (e.g., unmanned aerial systems, aerostats) to support communications in mobile environments. Airborne platforms can provide a mobile solution with rapid deployment capability when other communications are unavailable due to natural disasters, bandwidth constraints, or the operating environment.



Analysis: Public safety agencies should consider the following for mobile repeaters based on the communication system priorities (e.g., coverage area, number of users):

- Do users operate across a small or large geographic area?
- Are maritime or air-based assets used?
- Are there border restrictions to the system's operations (e.g., international)?
- Does the system operate on frequencies in accordance with FCC rules and regulations for signal power?



Cost: Mobile repeaters are priced in the \$-\$\$\$ range as an initial capital investment and require ongoing maintenance costs in the \$-\$\$ range.



Lifespan: Mobile repeaters typically have a lifespan of 11–15 years.

Physical Security Elements



Description: Physical security includes asset protection and threat assessment, detection, and containment. Threats include theft, vandalism, malicious intent to impair the system, and unauthorized access to equipment and network operations. Risks do not apply equally to different site types. For example, pole-mounted cabinet sites will have a different threat profile than full stand-alone shelters.



Function: Physical and electronic security elements protecting communications sites should be installed with consideration for potential threats (e.g., vandalism, theft, unauthorized access), which increases costs. Additional factors affecting cost include the type of access control system (e.g., fences, lock keys, electronic access cards, active detection systems). Additionally, the total network impact should be considered with “multi-function” sites, such as master sites, transport aggregation/hub sites, and shared sites requiring greater protection and hardening than smaller fill-in coverage sites. As such, any prioritization of physical security controls or resources should consider the larger impact to multi-function sites.



Usage: Mission critical operations require physical and electronic site monitoring elements.



Analysis: Public safety agencies should consider the following for physical and electronic site monitoring elements:

- Is there security or alarm system to detect unauthorized access, yet not impede legitimate maintenance?
- Is security fencing or exterior lighting required?
- Has shelter access been hardened with door alarms, deadbolts, and/or electronic access?
- Are remote cameras or a video recording system required?
- Do electronic access controls include user logins and various levels of access based on specific function to enhance equipment level security?



Cost: Costs vary widely depending on the element (e.g., fencing and remote camera costs depend on the site shape and size, electronic access control costs based on complexity of required functional access), generally priced in the \$–\$\$ range. Physical and electronic security elements require ongoing investment and sustainment costs in the \$–\$\$ range.



Lifespan: Physical and electronic security elements have a variable lifespan depending on the element (e.g., fencing has a longer lifespan than security cameras).

Note: Secure communications using encryption is covered in the [Features](#) section of this document.

Devices

Public safety agencies use multiple communications devices to meet their specific mission. Portable and mobile radios, cellular phones, and satellite phones deliver primary or backup communications in a variety of environments, scenarios, and emergencies. These devices have an optimal lifespan between 2–10 years. Additional factors affecting the lifespan of equipment include how the equipment is used (e.g., front line, back office); requirements or desire to migrate to a new technology; interoperability needs with a new or existing statewide or regional system; lack of replacement parts; and cost of maintenance or upgrades outweighing cost of purchasing new equipment.

Portable and Mobile Radios



Description: Handheld portable radios are typically carried by individual public safety personnel and tend to have a limited transmission range. Mobile radios are often located inside vehicles and use the vehicle’s power supply and a larger antenna, providing a greater transmission range than handheld portable radios.



Function: Public safety grade portable and mobile radios should be digital or analog capable, operate in assigned spectrum frequencies, support conventional or trunked systems, and be compatible with technical standards-based communications systems (e.g., P25 for LMR, LTE for broadband/IP-based technologies).



Usage: Users may require one or both types of radios with advanced features. For example, law enforcement officers may require standards-based encrypted portable and mobile radios that provide robust security and interoperability with devices that are encrypted in the same way (e.g., federal law enforcement partners). Firefighters and HAZMAT personnel require intrinsically safe radios to work in chemical plants, which can be an explosive environment. Additionally, ruggedized modes such as those built to military specifications may extend the longevity of services allowing operations in difficult environments such as water and fire/rescue operations. Conversely, the use of a device with minimal features/functions may prove to be an economical solution for public safety users that serve single agency missions that don’t require interoperability with other neighboring systems.



Analysis: Public safety agencies should consider the following for portable and mobile radio equipment based on the user’s position and responsibilities:

- What are the broader interoperability requirements in the area’s strategic plan (e.g., [Statewide Communication Interoperability Plan](#) [SCIP])? Will the user communicate across multiple systems in different operational modes and frequency bands?
- In the typical operating environment, will the user encounter excess water, sand, dust, vibration, shock, temperature, or an explosive environment?
- Do communications need to be secure? Does the user require advanced encryption standard (AES) capabilities?
- Will the user require wireless firmware and codeplug updates?



Cost: Portable and mobile radios are priced in the \$–\$\$ range as an initial capital investment and require ongoing maintenance costs in the \$ range.



Lifespan: Public safety grade portable and mobile radios typically operate for a lifespan of 7–10 years with proper maintenance.

Cellular Phones



Description: Cellular or mobile phones are handheld and "ultraportable" communications and computing devices with connectivity. These devices include a variety of platforms such as smart phones, netbooks, tablets, and pad devices.



Function: While voice capabilities are available through commercial broadband networks, LMR has been used by public safety for many years as the most reliable means of tactical communications and provides the most reliable means of voice communications at this time. Cellular phones are not designed to meet public safety grade requirements.



Usage: Many public safety agencies use commercial cellular data services or wireless broadband services to augment LMR capabilities. For example, law enforcement officers use situational awareness applications (e.g., Android Tactical Assault Kit) to review positioning, terrain, weather, and file sharing in real-time. Conversely, public works' personnel may find that low-cost cellular phones provide sufficient capability to support road work activities.



Analysis: Public safety agencies should consider the following for cellular phones based on the user's position and responsibilities:

- Do you need priority communications during major incidents or emergencies?
- Are communications typically between only two users?
- Is text messaging required?
- Is real-time situational awareness capability required with multi-jurisdictional responders?
- Are simultaneous voice and data capabilities required?
- Is access to the FirstNet Authority's NPSBN and other broadband services required? Do you know the contact or process to elevate users to primary access?
- Do you have access to [Government Emergency Telecommunications Services \(GETS\)](#)/[Wireless Priority Services \(WPS\)](#)?



Cost: Cellular phones are priced in the \$ range as an initial capital investment and require ongoing maintenance and repairs (e.g., software updates, replace cracked screen).



Lifespan: Cellular phones have a lifespan of 2–4 years given rapid technological advancements.

Satellite Phones



Description: Satellite phones are handheld devices that operate like cellular phones with connectivity provided by satellite service providers vice terrestrial based systems.



Function: Satellite phones offer a reliable alternative to land-based communications systems that may be unavailable or unreliable during natural or man-made disasters. Additionally, some systems have dispatch or push-to-talk capabilities (e.g., one-to-many) like LMR systems. Satellite phones are not designed to meet public safety grade requirements.



Usage: Satellite phones provide services where LMR or cellular networks are unavailable. For example, a public works' team may use a satellite phone in a waterproof case when working in a remote location outside of their systems coverage area. Similarly, law enforcement officers may use satellite phones when supporting maritime operations in lakes and offshore with minimal coverage.



Analysis: Public safety agencies should consider the following for satellite phones based on the user's position and responsibilities:

- Are primary systems damaged or overloaded due to manmade or natural disasters?
- Will users have a line-of-sight to the satellite or an outside antenna to ensure effective communications?
- Are international or cross-border calls required?
- Is the satellite phone use a long-term solution?
- Are data capabilities and features a primary requirement?



Cost: Satellite phones are priced in the \$ range as an initial capital investment and require ongoing service costs/fees, which are generally higher than cellular phone service costs/fees.



Lifespan: Satellite phones have a lifespan of 3–5 years.

Mobile Data Devices



Description: Mobile data devices are computerized devices (e.g., laptops, tablets) installed in vehicles to provide connectivity with dispatch and central computer systems.



Function: Mobile data devices are installed within vehicles using mounting systems, antenna connections, and consideration for potential hazards (e.g., vibration, shock). Additional factors affecting costs include weight, size, readability, accessibility (e.g., touchscreen), computing power, and compatibility with communications systems.



Usage: Many public safety entities use mobile data devices to perform routine, daily operations. Mobile data devices help responders to communicate with each other, retrieve information from databases (e.g., the Law Enforcement Agencies Data System), and augment mission critical voice capabilities. For example, law enforcement patrol vehicles receive routine dispatches, run wants, warrants, mapping, and motor vehicle checks using these devices, and some provide car-to-car messaging.



Analysis: Public safety agencies should consider the following for mobile data devices based on the user's position and responsibilities:

- Are commercial or private data services available with adequate bandwidth?
- In the typical operating environment, will the user encounter excess water, sand, dust, vibration, or shock?
- Does the user require data communications with multiple agencies?
- Are picture or video capabilities required?
- Is WiFi capable equipment required?
- Is vehicle power or only battery power available?



Cost: Mobile data devices are priced in the \$–\$\$ range as an initial capital investment and require ongoing maintenance and possible regular service costs/fees for network connectivity.



Lifespan: Mobile data devices have a lifespan of 3–10 years.

Accessories

Equipment accessories assist public safety users to comfortably perform their duties while maintaining access to communications. Commonly-used accessories include holsters, chargers, speakers, lapel microphone extensions, Bluetooth, vehicle kits, aircards, and intercoms. While costs vary, accessories are generally priced in the \$–\$\$ range as an initial capital investment and require minimal maintenance costs. Accessories have an optimal lifespan between 2–10 years depending on how the equipment is used (e.g., front line, back office). This document will briefly review function and analysis considerations for holsters, battery chargers, and speakers/microphones/intercoms. Public safety agencies should apply similar value analysis when evaluating other accessories.

Holsters



Function: Public safety holsters range from simple belt clips and leather carry cases, to swivel and fixed loop. Plastic belt clips provide a low-cost solution for back office applications such as dispatch rooms. Swivel holsters allow increased movement while fixed loop holsters provide for sturdy public works' applications.



Analysis: Public safety agencies should consider the following for holsters based on the user's position and responsibilities:

- What degree of movement and protection is required?
- Will the user encounter excess water, sand, dust, heat, vibration, or shock in typical operating environment?

Battery Chargers



Function: Chargers range from low-cost single battery or multi-battery models with a diagnostic tool (e.g., alerting when replacement is required), to vehicle and portable chargers for travel.



Analysis: Public safety agencies should consider the following for battery chargers based on the user's position and responsibilities:

- How many batteries need to be charged at a time?
- How quickly do batteries need to be charged?
- Is vehicle power available?

Speakers / Microphones / Intercoms



Function: Speakers, microphones (mics), and intercoms are designed to meet unique public safety needs including noise cancellation, suppression reducing background noise, and waterproofing for firefighters, covert law enforcement, and maritime operations. Public works personnel may require headsets that protect hearing in extreme or consistently loud environments. Specific accessories (e.g., programming, cloning cables, wireless speaker/mic) are often used within encapsulated hazmat suits where access to radio equipment is restricted. Intercoms are used for personnel in close proximity, such as within a firetruck or ambulance.



Analysis: Public safety agencies should consider the following for speakers/mics/intercoms based on the user's position and responsibilities:

- In the typical operating environment, will the user encounter excess noise, water, sand, dust, heat, vibration, or shock?
- Does the microphone require push-to-talk or voice activation?
- Are exaggerated controls required to operate effectively?
- Is WiFi or Bluetooth capable equipment required?
- Is vehicle power or only battery power available?

Features

Public safety personnel require equipment that offers a basic level of operability, interoperability, and reliability with other responders, coupled with various features and options based on their position and responsibilities. Features should be standards-compliant to minimize any interoperability challenges with communications systems and equipment. Two features—encryption and ruggedization—are key considerations for all emergency responders. Generally, these features drive up costs of communications systems and equipment while adding functionality, as well as encryption increasing security and ruggedized devices increasing lifespan of devices.

Encryption



Function: To protect against security risks and act on vulnerability assessments, public safety agencies secure equipment, information, and capabilities from physical and virtual threats. Examples of security risks include eavesdropping and unwanted disclosure of information. Encryption services protect sensitive information transmitted over wireless systems.

To minimize the possibility of sensitive information being monitored with low-cost equipment that is readily available or easily acquired, several choices of encryption are available for use in public safety equipment. Standards compliant algorithms, such as the AES, offer interoperability and a high level of protection. All federal public safety agencies are transitioning to AES. State, local, tribal, and territorial public safety agencies will need AES equipment to communicate securely with federal agencies.



Analysis: Public safety agencies should consider the following for encrypted mission critical communications based on the user's position and responsibilities:

- Does your agency operate on a P25 digital wireless communications network?
- Does the user require secure data communications?
- Does the user require secure interoperable communications with other agencies? Are those agencies capable of securing communications with the same encryption method?
- Is over-the-air-rekeying (OTAR) required?

Agencies identify specific needs for secure communications and implement encryption in a consistent manner and in collaboration with other public safety agencies. Successful encrypted communication requires all agencies understand how the use and coordination of encryption can affect interoperability.

Ruggedization



Function: Ruggedized systems and equipment are developed and tested to ensure reliant and resilient services remain available even under severe conditions. Manufacturers exhaustively test ruggedized equipment to meet P25 performance and interoperability specifications and meet public safety grade expectations.



Analysis: Public safety agencies should consider the following to determine need for ruggedized equipment based on the user's position and responsibilities:

- Will the user encounter excess noise, water, sand, dust, heat, vibration, or shock?
- Will the user be encumbered by protective gear or gloves when using?

Software and Data Storage

Communications systems and associated data storage equipment often have IP-based elements (e.g., programmable radios, ability to interface with a computer, databases/services on private intranets or the Internet). These features and functions are helpful to communications managers but come with an additional cost. Software is continually upgraded, and new features and protections added. In turn, equipment with software needs to be upgraded with the latest versions as released to ensure security features are installed, and the equipment is compatible with other similar equipment.

Additionally, public safety personnel collect an increasing variety and volume of data (e.g., body camera videos, 911 call information). This data is invaluable to public safety personnel but must be properly stored for analysis and future retrieval. Data storage equipment can be onsite servers or cloud-based solutions. Increased data storage capacity increases costs as well.

Software and Data Storage



Function: Public safety agencies continuously monitor and install software upgrades to maintain functionality and services. Software version upgrades are often sequential and require installation of all intermediary versions. Failure to upgrade software in a timely manner may lead to potential downtimes, extensive costs, inability to access stored data, and unnecessary exposure to security threats.



Analysis: Public safety agencies should consider the following when reviewing operations and maintenance of software and data storage:

- Does your agency have any software license fees?
- Does your agency incur monthly/annual maintenance costs for software upgrades?
- Does your agency identify and prioritize cybersecurity improvements using the [*National Institute of Standards and Technology \(NIST\) Cybersecurity Framework*](#)?
- Does your agency require data storage (i.e., local server or cloud-based)?

RECOMMENDATIONS

This *Emergency Communications Systems Value Analysis Guide* provides considerations to assist public safety agencies determine whether proposed communications systems and equipment are cost effective and offer the right value. With all budgeting decisions, cost and value can be a trade-off. Agencies must assess user requirements and identify unnecessary costs or potential savings through informed investments. Once identified, agencies should enact procedures to remove unnecessary costs and invest in right-sized solutions. Public safety guidance and technical assistance are available to assist with these actions.



Follow SAFECOM and NCSWIC Guidance developed by Experienced Public Safety Officials. Agencies should reference additional guidance resources on the [SAFECOM and NCSWIC website](#). Through collaboration with emergency responders and policy makers across all levels of government, SAFECOM, NCSWIC, and partner organizations created resources and guidance to improve public safety interoperability. The library is organized by elements of the Interoperability Continuum (i.e., Governance, Standard Operating Procedures, Technology, Training and Exercises, and Usage), as well as sections on planning, funding, interoperability, field operations guides, public safety software tools, and mobile applications. SAFECOM and NCSWIC work with federal communications programs and key stakeholders to develop better technologies and processes for the multi-jurisdictional and cross-disciplinary coordination of existing communications systems and future networks.



Request Technical Assistance. CISA provides all 56 states and territories with on-site technical assistance at no cost through the [Interoperable Communications Technical Assistance Program](#). These services include instruction and assistance with the planning, governance, operational, and technical aspects of developing and implementing interoperable communications initiatives. Technical Assistance offerings are designed to help emergency responders continue to communicate during disasters or large-scale planned events. Collaborate with your Statewide Interoperability Coordinator⁶ or tribal point of contact to submit technical assistance requests to CISA.

⁶ NCSWIC maintains a list of the Statewide Interoperability Coordinators or an acting representative from each state or territory in the designated region at: <https://www.dhs.gov/safecom/ncswic-membership>.

CONCLUSION

Communications investments are among the most significant, substantial, and long-lasting capital expenditures that public safety agencies make. There is no simple solution for determining emergency communications systems and equipment, and components require continuous investments to maintain services and replace parts. Procurement decisions require extensive assessments to identify user requirements, system components, and features that are cost effective and offer the right value. This assessment process to inform planning and cost estimation continues through the entire system lifecycle—beginning with initial capital investments, through ongoing maintenance and operations, replacement parts, and finally disposition and transition to new capabilities once a system has reached its useful end-of-life. Public safety agencies must also balance financial challenges to keep pace with the rapid technological advancements in an era of competing priorities and constrained resources. With these realities in mind, Governors, elected officials, and leaders should collaborate with Statewide Interoperability Coordinators and other state-level planners (including tribal or territorial leaders if applicable) to understand emergency communications capabilities and needs in their area, then incorporate that knowledge into planning and budgeting decisions.

About SAFECOM and NCSWIC

SAFECOM is comprised of more than 70 members representing federal, state, local, and tribal emergency responders, and major intergovernmental and national public safety associations, who aim to improve multi-jurisdictional and intergovernmental communications interoperability through collaboration with emergency responders and policymakers across federal, state, local, tribal, territorial, and international partners. SAFECOM members bring years of experience with emergency communications during day-to-day operations, and natural and man-made disasters. SAFECOM members offer insight and lessons learned on governance, planning, training, exercises, and technologies, including knowledge of equipment standards, requirements, and use. SAFECOM members also provide input on the challenges, needs, and best practices of emergency communications, and work in coordination with Department of Homeland Security to share best practices and lessons learned with others.

NCSWIC is comprised of Statewide Interoperability Coordinators and their staff from the 56 states and territories. NCSWIC assists states and territories with promoting the critical importance of interoperable communications and sharing best practices to ensure the highest level of interoperable communications within and across states and with their international partners along the borders.

SAFECOM and NCSWIC developed the *Emergency Communications System Value Analysis Guide* with support from CISA. This document reflects the expertise and knowledge of SAFECOM and NCSWIC members, and coordination efforts of CISA in bringing stakeholders together to share technical information, best practices, and lessons learned in funding and deploying public safety communications systems. Questions on this document can be sent to: SAFECOMGovernance@hq.dhs.gov and NCSWICGovernance@hq.dhs.gov.

APPENDIX: VALUE ANALYSIS CHECKLIST

The Value Analysis Checklist summarizes analysis questions throughout the [Systems Components](#) section of the *Emergency Communications Systems Value Analysis Guide*. This tool is designed to assist public safety agencies evaluate communications systems and equipment for cost effectiveness and value to its users. By answering the analysis questions, an agencies’ user requirements and unique missions will inform planning and budgeting decisions and result in cost effective investments that offer the right value.

Project management teams considering replacing or purchasing system components should also reference the [Emergency Communications System Lifecycle Planning Guide](#) for best practices, considerations, and additional checklists for each phase of the system lifecycle. These documents were developed by public safety officials and experts who have successfully managed communications systems across the Nation—from initial planning through final disposition.

Checklist: Value Analysis by System Components	
<input type="checkbox"/>	<p>Infrastructure – Towers</p> <ul style="list-style-type: none"> – What existing infrastructure or resources can you lease or share with other organizations rather than developing new communication sites? – What environmental impact statements (EIS) or environmental assessments (EA) are required? Will the selected site comply with Environmental Planning and Historic Preservation (EHP) and National Environmental Policy Act (NEPA) requirements? – Have the appropriate Federal Aviation Administration (FAA) requirements for height (i.e., above ground level), warning lights for aircraft, grounding requirements, and licensing requirements been addressed for the tower? – Have all necessary and appropriate permissions been received before construction begins? – Has a media and public communications plan been developed for a new radio tower site? – Is an adequate lightning protection system in place? Are physical security and safety measures included?
<input type="checkbox"/>	<p>Infrastructure – Shelters</p> <ul style="list-style-type: none"> – Is there adequate space for the shelter and access to the shelter? – In the operating environment, will you encounter excess water, sand, dust, heat, or cold? What heating, ventilation, and air conditioning (HVAC) capabilities are required? – Can the site be adequately secured from vandalism and unauthorized access? What level of access control is possible? – Does the shelter have adequate interior space for planned equipment and room for expansion? – Does the shelter have an adequate monitoring system for tower lighting, power systems, and environmental and security controls? – Have specific requirements (e.g., U.S. Department of Labor Occupational Safety and Health Organization), electrical codes, industry standards (e.g., Underwriters Laboratory), and manufacturer guidance been addressed to ensure the safety, security, reliability, and operability of the communications systems?
<input type="checkbox"/>	<p>Infrastructure – Commercial and Backup Power Equipment</p> <ul style="list-style-type: none"> – Is commercial power available or economically accessible? – Is commercial and backup power suitably sized for all users? – Is there sufficient space for backup power generation in or outside the shelter? – What is the impact if the communications site was not operating due to a power loss? – Are both short- and long-term backup power sources needed? – Are adequate fuel supplies accessible? – Are start testing and load testing regularly scheduled and accomplished? – Are your power systems monitored and alarmed?

Checklist: Value Analysis by System Components	
<input type="checkbox"/>	<p>Infrastructure – Transmission and Wired Lines</p> <ul style="list-style-type: none"> – In the operating environment, will lines encounter excess water, sand, dust, heat, or cold? Is an ice bridge required to protect lines or cables installed above ground? – Can routing over more than one physical path be accomplished to provide route diversity? – Will connections to other backbone networks be practical from the site? – Are protective and restorative measures available if services are lost or congested (e.g., Continuity Planning Suite, Telecommunications Services Priority [TSP])?
<input type="checkbox"/>	<p>Fixed Station Equipment – Antennas</p> <ul style="list-style-type: none"> – In the operating environment, are additional structural supports required? – Was an impact analysis performed when adding a new antenna to a tower? – Was the antenna properly grounded to protect from lightning? – Are Federal Communication Commission (FCC) guidelines followed for safe operation? – Are antenna systems adequately documented?
<input type="checkbox"/>	<p>Fixed Station Equipment – Repeaters and Towers on Wheels</p> <ul style="list-style-type: none"> – Do repeaters have the capability for remote management? – Will repeaters need to transmit encrypted signals? – If temporary deployment is required where coverage is intermittent or unavailable, does the equipment offer a low power configuration, portability, and ruggedization?
<input type="checkbox"/>	<p>Fixed Station Equipment – Console Equipment</p> <ul style="list-style-type: none"> – What type of system technologies will the console equipment service (e.g., 911, land mobile radio [LMR], Voice over Internet Protocol [IP], long-term evolution [LTE])? – What is the planned usage (e.g., 24/7 dispatch, backup or temporary)? – What programs and software will need to be integrated (e.g., records database)? – Do communications need to be secured/encrypted? – Is there a need to manage operations from a remote location or provide backup operations for another dispatch location? – Can dispatch requirements be consolidated across multiple jurisdictions? – Does your agency require audio recording capabilities?
<input type="checkbox"/>	<p>Fixed Station Equipment – Mobile Repeaters</p> <ul style="list-style-type: none"> – Do users operate across a small or large geographic area? – Are maritime or air-based assets used? – Are there border restrictions to the system’s operations (e.g., international)? – Does the system operate on frequencies in accordance with FCC rules and regulations for signal power?
<input type="checkbox"/>	<p>Fixed Station Equipment – Physical Security Elements</p> <ul style="list-style-type: none"> – Is there security or alarm system to detect unauthorized access, yet not impede legitimate maintenance? – Is security fencing or exterior lighting required? – Has shelter access been hardened with door alarms, deadbolts, and/or electronic access? – Are remote cameras or a video recording system required? – Do electronic access controls include user logins and various levels of access based on specific function to enhance equipment level security?

Checklist: Value Analysis by System Components	
<input type="checkbox"/>	<p>Devices – Portable/Mobile Radios</p> <ul style="list-style-type: none"> – What are the broader interoperability requirements in the area’s strategic plan (e.g., Statewide Communication Interoperability Plan [SCIP])? Will the user communicate across multiple systems in different operational modes and frequency bands? – In the typical operating environment, will the user encounter excess water, sand, dust, vibration, shock, temperature, or an explosive environment? – Do communications need to be secure? Does the user require advanced encryption standard (AES) capabilities? – Will the user require wireless firmware and codeplug updates?
<input type="checkbox"/>	<p>Devices – Cellular Phones</p> <ul style="list-style-type: none"> – Do you need priority communications during major incidents or emergencies? – Are communications typically between only two users? – Is text messaging required? – Is real-time situational awareness capability required with multi-jurisdictional responders? – Are simultaneous voice and data capabilities required? – Is access to the FirstNet Authority’s Nationwide Public Safety Broadband Network (NPSBN) or other public broadband services required? Do you know the contact or process to elevate users to primary access? – Do you have access to Government Emergency Telecommunications Services (GETS)/Wireless Priority Services (WPS)?
<input type="checkbox"/>	<p>Devices – Satellite Phones</p> <ul style="list-style-type: none"> – Are primary systems damaged or overloaded due to manmade or natural disasters? – Will users have a line-of-sight to the satellite or an outside antenna to ensure effective communications? – Are international or cross-border calls required? – Is the satellite phone use a long-term solution? – Are data capabilities and features a primary requirement?
<input type="checkbox"/>	<p>Devices – Mobile Data Devices</p> <ul style="list-style-type: none"> – Are commercial or private data services available with adequate bandwidth? – In the typical operating environment, will the user encounter excess water, sand, dust, vibration, or shock? – Does the user require data communications with multiple agencies? – Are picture or video capabilities required? – Is WiFi capable equipment required? – Is vehicle power or only battery power available?
<input type="checkbox"/>	<p>Accessories – Holsters</p> <ul style="list-style-type: none"> – What degree of movement and protection is required? – In the typical operating environment, will the user encounter excess water, sand, dust, heat, vibration, or shock in typical operating environment?
<input type="checkbox"/>	<p>Accessories – Battery Chargers</p> <ul style="list-style-type: none"> – How many batteries need to be charged at a time? – How quickly do batteries need to be charged? – Is vehicle power available?

Checklist: Value Analysis by System Components	
<input type="checkbox"/>	<p>Accessories – Speakers/microphones/intercoms</p> <ul style="list-style-type: none"> – In the typical operating environment, will the user encounter excess noise, water, sand, dust, heat, vibration, or shock? – Does the microphone require push-to-talk or voice activation? – Are exaggerated controls required to operate effectively? – Is WiFi or Bluetooth capable equipment required? – Is vehicle power or only battery power available?
<input type="checkbox"/>	<p>Features – Encryption</p> <ul style="list-style-type: none"> – Does your agency operate on a Project 25 digital wireless communications network? – Does the user require secure data communications? – Does the user require secure interoperable communications with other agencies? Are those agencies capable of securing communications with the same encryption method? – Is over-the-air-rekeying (OTAR) required?
<input type="checkbox"/>	<p>Features – Ruggedization</p> <ul style="list-style-type: none"> – In the typical operating environment, will the user encounter excess noise, water, sand, dust, heat, vibration, or shock? – In the typical operating environment, will the user be encumbered by protective gear or gloves when using?
<input type="checkbox"/>	<p>Software and Data Storage</p> <ul style="list-style-type: none"> – Does your agency have any software license fees? – Does your agency incur monthly/annual maintenance costs for software upgrades? – Does your agency identify and prioritize cybersecurity improvements using the National Institute of Standards and Technology (NIST) Cybersecurity Framework? – Does your agency require data storage (i.e., local server vs. cloud-based)?