



SAFECOM<sup>®</sup> NCSWIC<sup>®</sup>



# Understanding the Value of Public Safety Communications Systems

*A Brochure for Elected Officials and Decision-Makers*

---

April 2020

# Understanding the Value of Public Safety Communications Systems and Equipment

All public safety agencies, regardless of size or discipline—law enforcement, fire, emergency medical services, public works/utilities, and public safety answering points/dispatch centers—must be ready to serve and protect their citizens. Agencies build and maintain public safety communications systems and equipment to meet their unique needs. Emergency responders require a basic level of operability, interoperability, and reliability with other responders, along with various features for security and accessories based on their position and responsibilities. Additional features and accessories drive up costs, but are essential for many responders to effectively complete their mission.

However, not all system users need every feature or accessory, allowing agencies to save costs where possible. 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. Different disciplines assess their unique needs by conducting a value analysis of possible equipment to inform communications investments.

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. Agencies can then enact procedures to remove these unnecessary costs and stretch public safety funding to encompass only mission critical requirements.

## Key Considerations

Before conducting a value analysis on communications systems and equipment, agencies 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.

- Public safety agencies have mission critical requirements to support time-sensitive and lifesaving tasks. Infrastructure equipment, user devices, and methods of deployment must be appropriately 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 to remain fully-functional in all-hazards environment, during and immediately following all emergency response operations.**
- Communications systems must fulfill the jurisdiction's specific communications needs, as well as employ technical standards to ensure operability, promote interoperability, and provide protection from isolation and obsolescence. This includes purchasing standards-based equipment for all communications technologies and investing in digital encryption for security. **While technology is not the sole component of ensuring interoperable communications, it is a major facilitator of interoperability and standards that help make it work.**<sup>1</sup>

---

<sup>1</sup> For information on ensuring all components of interoperable communications (i.e., Governance, Standard Operating Procedures, Technology, Training and Exercises, and Usage), reference the [Interoperability Continuum](#) on the SAFECOM website.

- 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.**
- 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. **Communications investments and sustainment should be included in every year's budget.**
- In addition to the Federal Government allocating funding for the First Responder Network Authority's Nationwide Public Safety Broadband Network, the public safety community will continue to rely on land mobile radio (LMR) as the most reliable means of tactical communications and integrate capabilities for years to come. Sustainment of LMR 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 something from failing; and user support for answering operational questions. **Agencies must continue to sustain these services for effective LMR system operation.**
- Systems are comprised of a variety of interconnected components, each with their own optimal lifespan. For example, the general lifecycle length of handheld devices (e.g., 2–10 years) is far shorter than fixed station equipment and infrastructure (e.g., 7–25 years). Agencies must 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 to maintain communications functionality.**
- Agencies place personnel at risk 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 the entire network and data. Outdated equipment may also inhibit full functionality of newer technologies due to data capabilities or other features. **Maintaining outdated equipment may eventually become costlier than investment in new systems or equipment.**
- Public safety comprises multiple disciplines across all levels of government, the private and non-profit sectors, as well as interactions with citizens, requiring integrated operations to communicate. To ensure communications projects are compatible, interoperable, and support statewide plans and strategies, agencies 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 communications and understanding existing and planned investments across the region. **It is recommended agencies identify and share resources with public safety partners, which result in cost savings for the community.**
- Establishing interoperability between existing critical communications networks and evolving technologies is another way to promote efficiencies. Agencies across all levels of government should consider the Shared Communication Systems and Infrastructure (SCSI) approach to more effectively share infrastructure, equipment, and services in support of public safety communications.<sup>2</sup> SCSI benefits include improved spectrum use; optimized resource usage and management; streamlined operations; reduced capital, operations, and maintenance expenditures; and enhanced economies of scale. **Agencies are encouraged to use the SCSI approach to build communications networks that support multiple partners and disciplines.**

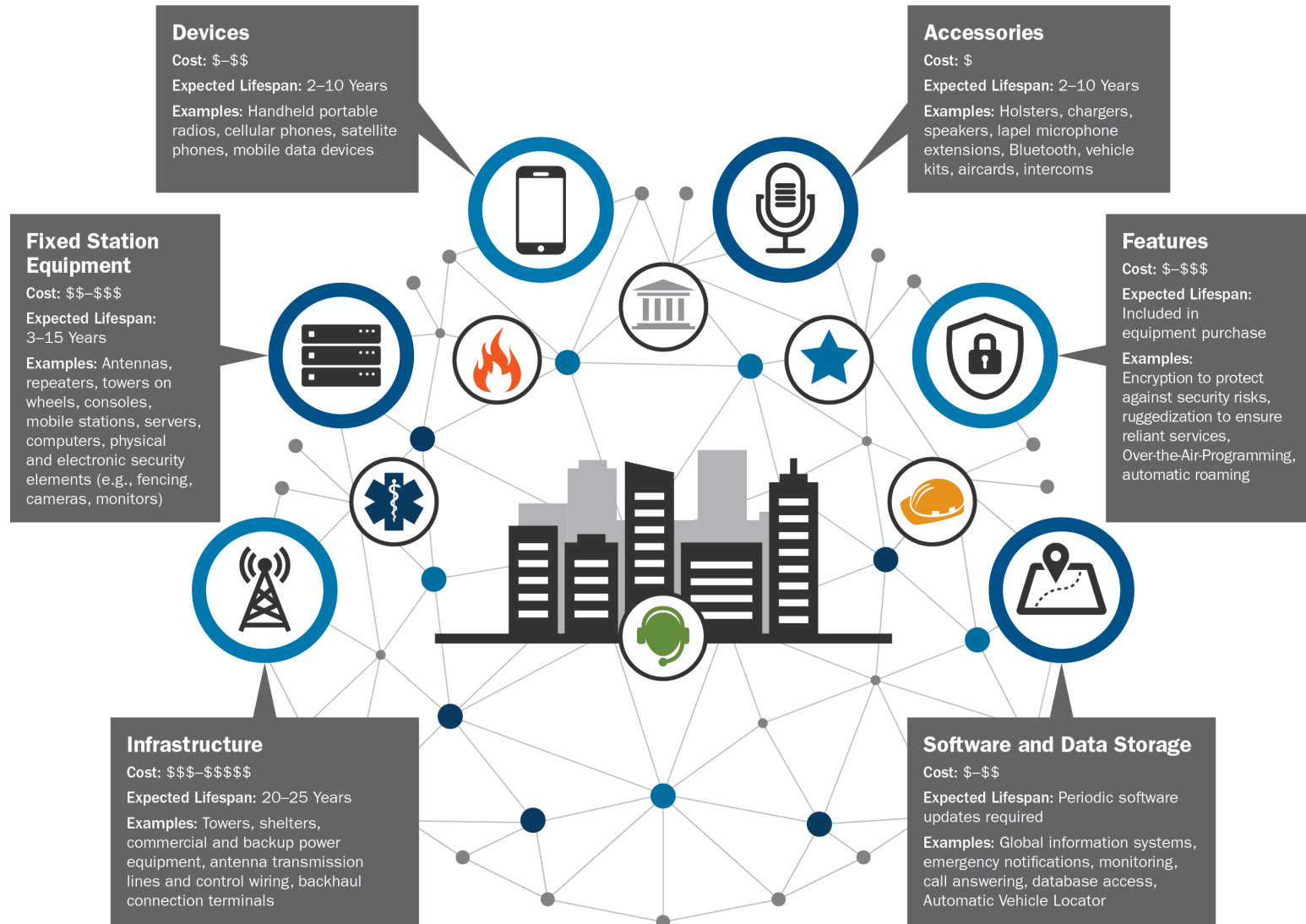
---

<sup>2</sup> 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. To learn more, visit <https://www.cisa.gov/scsi>.

# Communications System Components

System components are divided into six categories: Infrastructure, Fixed Station Equipment, Devices, Accessories, Features, and Software and Data Storage. **Figure 1** depicts common system components used by public safety agencies, cost ranges, and expected lifespan to illustrate the need for continuous investments. Cost ratings are relative to each other with Infrastructure being the most expensive and Accessories being one of the least expensive system components. Costs also vary depending on system configuration, owned or leased operation, geographic region, manufacturer, applicable technical standards testing, operational and maintenance costs, and other factors. When considering discipline-specific investments, infrastructure and fixed station equipment for public safety communications systems are generally the same regardless of size or discipline.

**Figure 1. Public Safety Communications System Components**



## Value Analysis Guide

In a climate of heightened competition for public safety funding, leaders make difficult budgeting decisions while addressing a variety of state and local 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. SAFECOM and the National Council of Statewide Interoperability Coordinators (NCSWIC), in collaboration with 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. The Guide 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 Guide provides a description, function, usage, analysis questions, costs, and expected lifespan of common system components used by public safety agencies, with considerations of key features based on the specific user's position and responsibilities. These features inform planning and cost estimation to include relative cost increases, potential savings, benefits, and risks, as well as applicability by discipline.



**Description:** Brief explanation of the system component and operation within a public safety communications system. Agencies may use these descriptions to inform decision-makers who are unfamiliar with components.



**Function:** Public safety agencies have mission critical requirements to support time-sensitive and lifesaving tasks. Thus, equipment must meet Public Safety Grade expectations and employ Technical Standards to offer operability, interoperability, resiliency, and security while in rigorous and harsh environments. Functionality, not cost, should be the driving factor in communications investments.



**Usage:** Public safety agencies can coordinate investments and share resources with partners. Additional cost savings may be achieved based on the specific user's position and responsibilities. For example, law enforcement officers may require standards-based encrypted radios that provide robust security and interoperability with partner agencies. Conversely, public works' personnel may find that low-cost cellular phones provide sufficient capability to support road work activities.



**Analysis:** To help assess user requirements and unique missions, the Guide lists questions for each component. For example, agencies should evaluate whether the user will encounter excess water, sand, dust, heat, vibration, or shock in typical operating environment, and thus require ruggedized devices.



**Cost:** Capital and ongoing maintenance costs are captured in ranges using \$-\$\$\$\$\$ designations and estimations are relative to each other. For example, infrastructure is the most expensive compared to accessories as one of the least expensive component. Costs vary depending on system configuration, owned or leased operation, geographic region, manufacturer, applicable technical standards testing, as well as operational and maintenance costs, and are often paid over multiple years.



**Lifespan:** Systems are comprised of a variety of interconnected components, each with their own optimal lifespan of approximately 2–25 years with proper maintenance. For example, devices may require replacement every 2 years, whereas fixed station equipment may operate for 15 years. The Guide outlines additional factors such as environmental, technological advancements, and equipment usage that affect lifespan.

With all budgeting decisions, cost and value can be a trade-off. The *Emergency Communications Systems Value Analysis Guide* offers recommendations and a Value Analysis Checklist to assist public safety agencies make these decisions. To start, agencies assess requirements and proposed solutions, then identify unnecessary costs or potential savings. Once identified, agencies should enact procedures to remove unnecessary costs and invest in right-sized solutions. [SAFECOM and NCSWIC](#) offer guidance resources developed by public safety officials and experts who have successfully managed communications systems across the Nation. The [CISA Interoperable Communications Technical Assistance Program](#) is also available to assist agencies with these actions.

## **About SAFECOM/NCSWIC**

SAFECOM is comprised of more than 70 members representing federal, state, local, and tribal emergency responders, and major intergovernmental communications interoperability through collaboration with emergency responders and policymakers. NCSWIC is comprised of Statewide Interoperability Coordinators and their staff from the 56 states and territories. Together, SAFECOM and NCSWIC collaborated with CISA to provide expertise and knowledge of technical information, best practices, and lessons learned in funding and deploying public safety communications systems. Send any questions on this document to [SAFECOMGovernance@hq.dhs.gov](mailto:SAFECOMGovernance@hq.dhs.gov) and [NCSWICGovernance@hq.dhs.gov](mailto:NCSWICGovernance@hq.dhs.gov).