National Emergency Communications Plan

September 2019

CISA
CYBER+INFRASTRUCTURE

This page intentionally left blank.

Message from the Director

The Department of Homeland Security's (DHS) commitment to ensuring a homeland that is safe, secure, and resilient against evolving threats and hazards is what has guided our work since its establishment in 2002. Ensuring operable and interoperable communications and real-time information sharing among responders during all threats and hazards is paramount to the safety and security of Americans. From a small-scale incident to a significant natural or manmade disaster, responders depend on the seamless flow of voice, video, and data communications to respond to and recover from events that threaten lives and property.

The National Emergency Communications Plan (NECP) is the Nation's roadmap to ensuring emergency communications interoperability at all levels of government. The Cybersecurity and Infrastructure Security Agency leads the effort to update and implement the NECP, but it requires participation from the whole community to be successful. Since the last NECP release in 2014, the emergency communications landscape has experienced unprecedented change. The frequency and complexity of emergencies are on the rise during a time when technology is advancing at a faster pace than any other time in history. While responders still rely heavily on land mobile radio for voice communications, comprehensive strategies for emergency communications must integrate the full Emergency Communications Ecosystem, including broadband, alerts and warnings, social media, and Next Generation 911.

Internet Protocol-based devices and applications have the potential to vastly improve emergency responder capabilities, yet also introduce new challenges such as cybersecurity threats, the need for a more technically skilled workforce, and shorter equipment lifecycles. The NECP emphasizes the need for strong governance structures, updated policies and procedures, as well as joint exercises and trainings to improve interoperability which ensures information is provided to the right people at the right time.

The 2019 NECP update was developed in partnership with Federal, state, local, tribal, and territorial jurisdictions and the private sector. We must work together to address the complex mission and achieve the NECP's stated vision to:

> ***Enable the Nation's emergency response community to communicate and share information securely across communications technologies in real-time, including all levels of government, jurisdictions, disciplines, organizations, and citizens impacted by any threats or hazards event.***

To that end, I thank those who contributed to the development of this Plan and ask for your continued cooperation and assistance as we implement the NECP. By working together will we make progress toward increasing the effectiveness and efficiency of emergency communications and information sharing and ultimately help protect the lives of our fellow Americans.

Christopher C. Krebs
Director, Cybersecurity and Infrastructure Security Agency

Table of Contents

Executive Summary

Every day in cities and towns across the Nation, emergency response personnel respond to incidents of varying scope and magnitude. Their ability to communicate in real time is critical to establishing command and control at the scene of an emergency, maintaining event situational awareness, and operating within a broad range of incidents. However, as numerous after-action reports and national assessments have revealed, there are still communications deficiencies that affect the ability of responders to manage routine incidents and support responses to natural disasters, acts of terrorism, and other incidents.

Recognizing the need for an overarching emergency communications strategy to address these shortfalls, Congress directed the Department of Homeland Security (DHS) Office of Emergency Communications—re-designated in 2018 as the Emergency Communications Division within the Cybersecurity and Infrastructure Security Agency (CISA)—to develop and periodically update the National Emergency Communications Plan (NECP). Title XVIII of the Homeland Security Act of 2002 (6 United States Code 101 et seq.), as amended, calls for DHS to develop the NECP in coordination with stakeholders from all levels of government and the private sector. DHS previously updated the plan in 2014. This publication is the second update.

DHS worked with stakeholders from federal, state, local, tribal, and territorial agencies, public safety associations, and the private sector to develop the NECP—a strategic plan that establishes a national vision for the future state of emergency communications:

To enable the Nation's emergency response community to communicate and share information securely across communications technologies in real time, including all levels of government, jurisdictions, disciplines, organizations, and citizens impacted by any threats or hazards event

The NECP establishes six strategic goals to drive progress toward the vision:

Goal 1: Governance and Leadership

Develop and maintain effective emergency communications governance and leadership across the Emergency Communications Ecosystem

Goal 2: Planning and Procedures

Develop and update comprehensive emergency communications plans and procedures that address the evolution of risks, capabilities, and technologies across the Emergency Communications Ecosystem

Goal 3: Training, Exercises, and Evaluation

Develop and deliver training, exercise, and evaluation programs that enhance knowledge and target gaps in all available emergency communications technologies

Goal 4: Communications Coordination

Improve effective coordination of available operable and interoperable public safety communications capabilities for incidents and planned events

Goal 5: Technology and Infrastructure

Improve lifecycle management of the systems and equipment that enable emergency responders and public safety officials to share information efficiently and securely

Goal 6: Cybersecurity

Strengthen the cybersecurity posture of the Emergency Communications Ecosystem

To meet these goals, the updated NECP establishes 19 objectives, each with success indicators, for the continued improvement of emergency communications for the Nation. Public safety agencies and partners should incorporate elements of these objectives into their federal, state, tribal, territorial, regional, jurisdictional, and local-level plans and measure progress until the associated success indicators have been achieved. By adopting these goals and objectives into their strategic plans, agencies support three national priorities for advancing emergency communications:

1. **Enhance effective governance across partners with a stake in emergency communications, embracing a shared responsibility of the whole community from traditional emergency responders and supporting entities to the citizens served;**
2. **Address interoperability challenges posed by rapid technology advancements and increased information sharing, ensuring the most critical information gets to the right people at the right time; and**
3. **Build resilient and secure emergency communications systems to reduce cybersecurity threats and vulnerabilities.**

Communications investments are among the most significant, substantial, and long-lasting capital expenditures that public safety agencies make. Stakeholders must balance **financial challenges** to keep pace with the rapid technological advancements in an era of reduced grant funding and constrained resources. Additionally, the whole community faces increasingly complex incidents and threat environment. Communication support must include the **integration and alignment of technologies** (e.g., land mobile radio, Next Generation 911, First Responder Network Authority's Nationwide Public Safety Broadband Network, as well as alerts, warnings, and notifications systems) and standard processes to support the interoperability of systems and services for information exchange among the responder and partner communities. With these realities in mind, CISA recognizes that the emergency response community will realize this national vision in stages, as agencies invest in new communications systems and technologies emerge.

The NECP provides guidance to those that plan for, coordinate, maintain, invest in, and use communications to support public safety operations. Given the diverse entities that are directly involved, supporting, or impacted by emergencies, the **Emergency Communications Ecosystem** includes the various functions and people that exchange information prior to, during, and after incidents and planned events. This includes traditional emergency responder disciplines (e.g., law enforcement, fire, emergency medical services, emergency communication centers/public safety answering points, emergency management) and other entities that share information during emergencies, such as medical facilities, utilities, nongovernmental organizations, as well as the media and private citizens. The Ecosystem is dynamic, depending on the incident or planned event, as well as multi-directional because anyone can initiate emergency communications. Although the individual responsible for coordinating emergency communications varies across jurisdictions, regions, and organizations, having an established central point of contact is critical for progressing emergency communications capabilities. Since the first NECP, states and territories have made strides in appointing a **Statewide Interoperability Coordinator** to serve as a central coordinator for emergency communications; however, not all have dedicated resources to this critical full-time position.

To implement the updated NECP, CISA will partner with the public safety community to identify strategies to accomplish the NECP's goals and objectives to improve nationwide emergency communications capabilities. CISA acknowledges that the Nation does not have unlimited resources

to address all deficiencies in emergency communications. Consequently, the NECP will be used to identify and prioritize investments to move the Nation toward this common vision.

The future of emergency communications is at a critical juncture. Through the NECP and the work of CISA and its partners, CISA is committed to supporting the Nation's emergency responders, including supporting organizations, decision makers, and citizens, as they strive to meet their missions and advance emergency communications. As required by Congress, the NECP is a living document subject to periodic review and updates by CISA in coordination with stakeholders. Future iterations will be revised based on progress made toward achieving the NECP's goals, variations in national priorities, and lessons learned from after-action reports.

NECP VISION

To enable the Nation's emergency response community to communicate and share information securely across communications technologies in real time, including all levels of government, jurisdictions, disciplines, organizations, and citizens impacted by any threats or hazards event.

Introduction

Emergency communications are critical to the Nation's ability to respond to devastating natural disasters, terrorist threats, and other emergency events, incidents, and routine activities affecting our communities every day. When faced with these situations, the public safety community has a collective responsibility to share information. Achieving this goal requires communications capabilities that are resilient and secure[1] today, yet agile enough to integrate advanced and emerging technologies tomorrow. This important component of national preparedness relies on coordinated input from the whole community, including individuals, the private sector, non-profits, and all levels of government (e.g., federal, state, tribal, territorial, regional, jurisdictional, and local).

Emergency Communications

The means and methods for exchanging information necessary for successful incident management

Since the establishment of Department of Homeland Security (DHS) in 2003, one of its top priorities has been to improve communications capabilities among the public safety community. The Department has partnered with emergency responder agencies to ensure access to reliable, secure, and interoperable communications at all times in order to save lives, protect property, safeguard the environment, stabilize communities, and meet basic human needs following an incident.

The Homeland Security Act of 2002 (6 U.S. C. § 1802) as amended, provided renewed focus and vitality to this critical homeland security mission. The legislation established the DHS Office of Emergency Communications, which was re-designated as the Emergency Communications Division within the Cybersecurity and Infrastructure Security Agency (CISA), to lead the development and implementation of a comprehensive approach to advancing national interoperable communications capabilities. To achieve this objective, the act required CISA to develop the National Emergency Communications Plan (NECP) to "provide recommendations regarding how the United States should support and promote the ability of emergency response providers and relevant government officials to continue to communicate in the event of disasters and to ensure, accelerate, and attain interoperable emergency communications nationwide."[2] Appendix 1 details how the NECP meets the statutory requirements.[3]

CISA collaborates closely with the public safety community to support and promote effective emergency communications through stakeholder-driven programs and services. Over the next 5 years, CISA will focus its efforts on implementing the goals and objectives articulated in the NECP. These critical components for advancing emergency communications fall under three national priorities: (1) to enhance effective governance across partners with a stake in emergency communications,

[1] For purposes of this document, *secure* refers to the confidence in confidentiality, integrity, and availability of communications, not to government sensitive or classified communications.
[2] Homeland Security Act of 2002 (6 U.S. C.§ 1802), as amended.
[3] Appendix 2 lists the NECP's key authorities.

embracing a shared responsibility of the whole community from traditional emergency responders and supporting entities to the citizens served; (2) to address interoperability challenges posed by rapid technology advancements and increased information sharing, ensuring the most critical information gets to the right people at the right time; and (3) to build resilient and secure emergency communications systems to reduce cybersecurity threats and vulnerabilities, as introduced through Internet Protocol (IP)-based technologies and services.

Purpose

As the Nation's strategic plan for emergency communications, the NECP establishes a vision ***to enable the Nation's emergency response community to communicate and share information securely across communications technologies in real time, including all levels of government, jurisdictions, disciplines, organizations, and citizens impacted by any threats or hazards event***. To achieve this vision, the NECP outlines 6 nationwide goals and 19 objectives to improve critical capabilities through partnerships, joint planning, and unified investments across levels of government. Its focus is to ensure the public safety community and citizens are collectively driving toward a common end-state for communications.

Development

To envision a desired future state, CISA examined current strategies, resource decisions, and investments for emergency communications and impacts from an ever-evolving environment. Through ongoing coordination with emergency responders, CISA reviewed the whole community's many accomplishments since the first NECP's publication in order to understand the remaining hurdles to be cleared.

> "The SAFECOM Nationwide Survey gives us a clear picture of where we are—as opposed to where we think we are—and identifies what to address to get where we want to be."
>
> **Sheriff Paul Fitzgerald**
> Story County Iowa, SAFECOM Member

CISA conducted the SAFECOM Nationwide Survey[4] and resulting 2018 Nationwide Communications Baseline Assessment, in which thousands of public safety agencies and organizations participated. Additionally, CISA used an extensive stakeholder engagement process to identify challenges and propose solutions to help improve emergency communications. As a result, representatives of major public safety organizations, government agencies, and key industry partners from the communications and information technology sectors recommended updating the NECP's vision, goals, and objectives to reflect current capability gaps and needed improvements.

[4] Information about the SAFECOM Nationwide Survey and results can be found at https://www.cisa.gov/safecom/sns.

Scope

The NECP serves as the Nation's strategic plan to improve emergency communications. It provides guidance to those that plan for, coordinate, invest in, and use communications to support response and recovery operations. This includes traditional emergency responder disciplines (e.g., law enforcement, fire, emergency medical services, emergency communication centers/ public safety answering points, and emergency management) and other partners that exchange information prior to, during, and after incidents and planned events.

Progress

In the 2018 Nationwide Communications Baseline Assessment, respondents across the targeted disciplines and levels of government indicated there was an overall strengthening of emergency communications since 2011. For example, more than 84 percent of state and territorial respondents reported significant or some improvement in the strengthening of their communications operability, interoperability, or continuity. While these results show progress, findings also reflected the need to address specific challenges, including emerging technologies (e.g., IP-based networks, next-generation data technologies); new capabilities (e.g., mobile data, public safety applications); and new partners (e.g., information technology departments, private sector infrastructure owners).

CISA has helped the public safety community implement the NECP through its programs, services, and guidance. CISA provides on-site technical assistance, training, and regional support at no cost to agencies, including instruction on the planning, governance, operational, and technical aspects of developing and implementing emergency communications.

Organization of the NECP

This update to the NECP supersedes the 2014 NECP update and is effective immediately. The plan is comprised of the following four sections:

- **Emergency Communications Ecosystem** explains the various people and functions that exchange information prior to, during, and after incidents and planned events.
- **NECP Strategic Goals** and associated objectives, establishes the strategy to meet the three national priorities and better position the whole community for the future of emergency communications. Figure 1 depicts a summary of the NECP's vision, goals, and objectives.
- **Implementing the NECP** describes CISA initiatives to develop an action plan and promotion campaign, measure progress through nationwide communications assessments, and report biennially to Congress.
- **Conclusion** recaps the plan's themes and key take-aways for emergency communications officials.

The included Annex expands upon the descriptions of the success indicators for the NECP goals and objectives. Appendices include the Statutory Requirements Matrix, Key Authorities, Roles and Responsibilities, the SAFECOM Interoperability Continuum, Source Documents, Glossary, and Acronyms.

Figure 1: Summary of NECP Goals and Associated Objectives

Emergency Communications Ecosystem

Since the NECP was first published in 2008, the public safety community has made significant strides to enhance governance structures, adopt common policies and procedures, expand training and exercise programs, migrate legacy systems, integrate new technologies, and mitigate the growing number of cyber threats. These efforts are not constrained within the limits of traditional emergency response of law enforcement, fire, emergency medical services, and emergency communication centers/public safety answering points. Instead, entities with different communications functions including supporting organizations, decision makers, and citizens rely on one another to exchange information prior to, during, and after incidents and planned events—a concept referred to as the Emergency Communications Ecosystem.

The public safety community continues to prioritize maintaining land mobile radio and data exchange systems, as well as improving operability, interoperability, and resiliency of communications capabilities. Emergency responders are also embracing emerging technologies and integrating them with existing systems. With the First Responder Network Authority's (FirstNet Authority) implementation of the Nationwide Public Safety Broadband Network, agencies will be able to supplement existing systems to provide public safety users with dedicated spectrum, added broadband capabilities, and advanced technologies to increase situational awareness. However, network integration presents new cybersecurity risks as a result of interconnected, IP-based technologies. It requires implementing effective strategies to enhance the resiliency of IP-based infrastructures and safeguard private or sensitive information transmitted across systems and devices, while also enabling response.

Response agencies are becoming more connected to additional sources of information during emergencies, such as medical personnel, critical infrastructure operators, and private citizens. While these individuals are not typically trained responders, they can share valuable information during response and recovery efforts. Additionally, because social media use is increasing, responders need to (1) develop best practices for engaging with the public to ensure accessibility to and for all citizens,[5] and (2) analyze social media to gain situational awareness in times of civil unrest, emergencies, and disasters. Agencies also face challenges retaining qualified communications personnel, securing adequate funding for ongoing operations and maintenance, and navigating complex and varying governance structures to formalize partnerships and establish resource sharing agreements.

[5] Considerations for responders and private citizens include disabilities and others with access and functional needs.

National Preparedness Goal

A secure and resilient Nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk

To organize the whole community toward the National Preparedness Goal, the National Response Framework and National Incident Management System guide how public safety responds to all types of emergencies. These guiding principles are built on scalable, flexible, and adaptable concepts for managing incidents that range from the serious but purely local to large-scale terrorist attacks or catastrophic natural disasters. They define roles, responsibilities, and coordinating structures for delivering core capabilities required to respond to an incident and how response efforts integrate with other preparedness mission areas, including prevention, protection, mitigation, and recovery.

> "The Emergency Communications Ecosystem must support the community's incident response role to make our Nation safer and more resilient as we face increasingly complex emergencies. The NECP prepares public safety to address today's challenges and plan for the future."
>
> **Ron Hewitt**
> Assistant Director for Emergency Communications, CISA

Incorporating the National Response Framework and National Incident Management System principles, the Emergency Communications Ecosystem is comprised of the various functions and people that exchange information prior to, during, and after incidents. The Ecosystem includes the breadth of organizations and individuals with roles in emergency communications, beyond traditional emergency responder disciplines, government agencies, and jurisdictional boundaries.[6] The Ecosystem is dynamic; not everyone is needed every day, depending on the incident or planned event. Being multi-directional, emergency communications can be initiated by anyone, including supporting entities or private citizens. The hypothetical scenario in Figure 2 illustrates response complexities (e.g., use of social media and citizen engagement) that are becoming more commonplace as the Emergency Communications Ecosystem evolves.

[6] Appendix 3: Roles and Responsibilities describes whole community partners, public and private, that are involved in the emergency communications mission.

Response Scenario

In a rural Mid-West town, the local police department noted a sudden increase in social media messages and postings on the community listserv complaining about abnormal numbers of people and vehicles present at all hours around a neighborhood. This volume of messages compounded by other calls to county government officials, the public works agency, and the volunteer fire department culminated in an initial investigation by local law enforcement, including targeted monitoring of social media traffic.

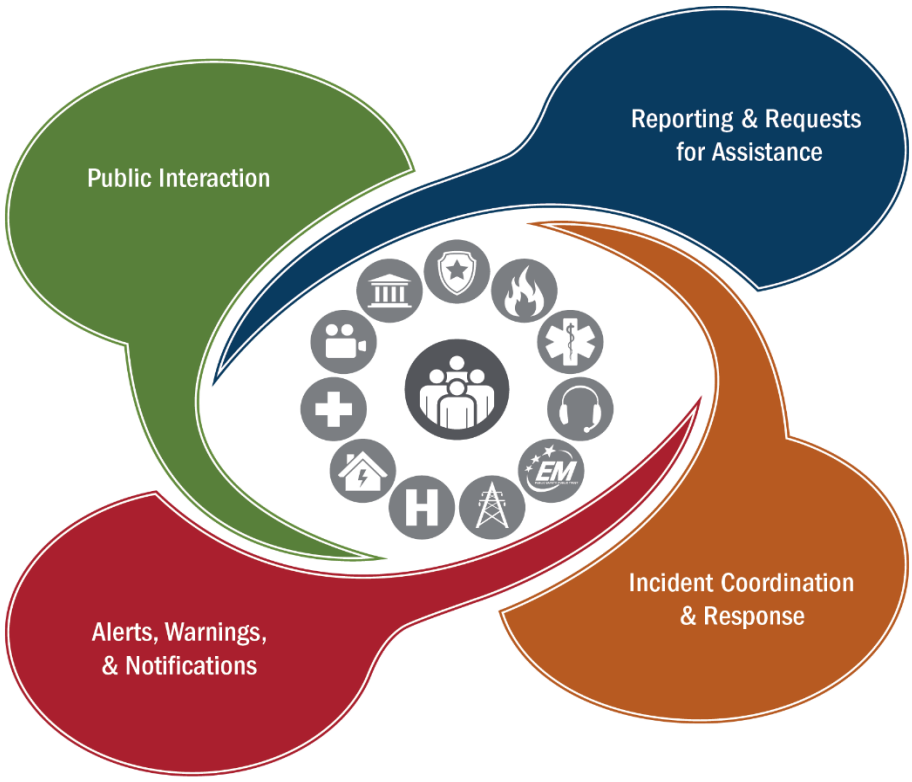
Bolstered by additional information from calls and text messages via 911 received by the emergency communications center/public safety answering point regarding reports of strange odors emanating from the area, local law enforcement alerted the regional drug task force of their suspicions of the existence of a clandestine drug lab. The task force investigation led to a search warrant. The task force, with members drawn from local police, the county sheriff's office, the state police, regional hazardous materials response team, and the U.S. Drug Enforcement Administration, coordinated movements with uniformed law enforcement personnel on encrypted interoperability radio channels and executed the search and arrest warrants. As they broke through the door of the unoccupied residence, the strong odor of toxic chemicals overwhelmed them, and as they backed out, they spotted some booby traps within steps of the entryway. Body cameras on the entry team members recorded the scene within the illicit lab, including details such as chemical components stockpiled in the residence and paraphernalia regarding booby trap construction. Additional resources were requested including the state bomb squad and more fire department units.

The unified or area command and the emergency communications center/public safety answering point dispatch personnel coordinated with uniformed law enforcement officers and fire officials to identify the safe zone in order to establish primary, secondary, and traffic perimeters and necessary detours and evacuations. The emergency communications center/public safety answering point used its public alert system to make calls and send short text messages to inform neighborhood residents of evacuation orders and shelter resources. The public information officer alerted the media and the public using social media and broadcast news resources about police activity, traffic disruptions, and a request to avoid the area. Mutual aid radio frequencies were used to coordinate response operations between responders. Fire apparatus, paramedics, and the bomb squad used geo-navigational aids to reach the scene and communicated via a common encrypted radio channel to coordinate their efforts. A command post and unified command were established, with personnel using FirstNet's Nationwide Public Safety Broadband Network to support communications, logistical needs, and gather various data inputs to formulate a common operating picture to effectively manage resources. This event would likely last all day.

Figure 2: Emergency Communications Ecosystem in Action

As illustrated in the scenario, communications functions within the Emergency Communications Ecosystem have become increasingly interwoven and complex. Figure 3 depicts key functions that are necessary to achieve reliable, secure, and interoperable emergency communications. This includes reporting and requests for assistance; incident coordination and response; alerts, warnings, and notifications; and public interaction.

The four communications functions in Figure 3 are represented as outer blades circling whole community partners. These partners represented in grey icons depict that anyone can initiate any function at any time, and how information flows multiple directions, depending on the nature of the event or incident. These primary functions, their purpose, and examples of each are listed below.



Communications Functions	Purpose	Examples
Reporting & Requesting Assistance	Urgent and non-urgent requests or information sharing made to public safety resources using defined emergency and non-emergency paths	911, 311, dedicated numbers, tip lines, alarm activated, face-to-face, triggered telematics system, social media, web applications, detection of service outages or disruptions
Incident Coordination & Response	Direct voice and data communications among public safety responders, emergency communication centers/public safety answering points, and emergency support systems to establish command and control, situational awareness, and shared common operating picture	Information sharing, joint planning, radio communications, in-field operations, data exchange
Alerts, Warnings, & Notifications	Instructional messages directing protective actions to save lives and property, and convey time-sensitive information for preparation, response, and recovery-related services	Active threats or civil dangers, hazmat, AMBER alerts, weather watches, fire warnings, evacuation orders, area accessibility updates, all-clear notices, Emergency Alert System, Wireless Emergency Alerts
Public Interaction	Public's sharing of information through various public or commercial networks supporting the Internet, social media, and telephony communications	Telephone calls, social media, such as Facebook, Twitter, web services and applications

Figure 3: Emergency Communications Ecosystem Key Communications Functions

NECP Strategic Goals

Goal 1: Governance and Leadership

Goal 2: Planning and Procedures

Goal 3: Training, Exercises, and Evaluation

Goal 4: Communications Coordination

Goal 5: Technology and Infrastructure

Goal 6: Cybersecurity

Goal 1: Governance and Leadership

Develop and maintain effective emergency communications governance and leadership across the Emergency Communications Ecosystem

Objective 1.1: Formalize governance through policy, documentation, and adequate funding

Objective 1.2: Structure more inclusive governance by expanding membership composition

Objective 1.3: Adopt adaptive governance strategies to address the rapid evolution of technologies, capabilities, and risks

Goal 1: Governance and Leadership

Effective coordination and decision making are critical first steps to ensuring successful emergency communications. Achieving this requires robust governance structures and processes designed to ensure accountability, inclusiveness, adaptability, and action. The strength of emergency communications governance is not measured by its ability to maintain the status quo, but to drive improvements in balance with the rapid evolution of technologies.

Public safety continues to expand its network of partners to include those involved in receiving and sharing information during both normal and emergency operations. Partnership coordination is further strengthened and verified by establishing formal decision-making bodies, gaining fiscal and legislative support from elected and appointed officials, creating consistent policy, and addressing regulatory change. Governance bodies benefit from the contributions of representatives from all organizations with a role in these operations, including those outside the realm of traditional response (e.g., transportation, public works, public health, utilities, natural resources or parks and recreation, and building inspectors). With the adoption and integration of new technologies, governance is an initial step toward preparing first responders to manage the benefits and risk of increased information exchange across organizations. Emergency communications governance remains the primary mechanism through which collaborating agencies establish processes and plans, determine and address capability gaps, and achieve progress toward interoperability.

Objective 1.1. Formalize governance through policy, documentation, and adequate funding

Formalized governance provides a unified approach to organize emergency communications across multiple disciplines, jurisdictions, and organizational functions. Written agreements, backed by formal governance, establish common goals and minimize risks for the communities they serve. Formal governance structures (e.g., Statewide Interoperability Governing Bodies, Statewide Interoperability Executive Committees, Statewide 911 Boards, and state-alerting authorities) provide a foundation for public safety entities to collaborate, plan, and make decisions on strategies and operations that mutually support the investment, sustainment, and advancement of communications-related initiatives. Establishing statewide governance or revising the functions of existing bodies through statutes or Executive Orders formalizes the group's authority to make funding recommendations supported through the state's general funds or federal grant allocations. A group's charter or bylaws also authorizes the group's existence and clarifies governance operations and roles on how to align its vision to longer-term strategies.

Robust governance establishes and maintains central coordination points or decision-making bodies to lead the management and administration of emergency communications systems and services, resource allocation and project prioritization, and collaboration necessary for achieving a strategic vision for interoperability.

> "Statewide Interoperability Coordinators are redefining their roles in this environment as the state's steward coordinating multiple technologies and systems—all of which need to be interoperable for our responders to do their jobs."
>
> **Joe Galvin**
> Illinois Statewide Interoperability Coordinator, National Council of Statewide Interoperability Coordinators Chair

Supporting Statewide Interoperability Coordinators

Since 2010, full-time Statewide Interoperability Coordinator positions have declined 70%, from 44 to 12 (see Figure 4). In the remaining states, the Statewide Interoperability Coordinator is a collateral duty or part-time position owing to funding constraints, which puts statewide interoperability programs at risk due to the lack of a dedicated coordination point. Decision makers rely heavily on Statewide Interoperability Coordinators to translate technical issues into policy and coordinate cost-effective solutions for maintaining legacy systems and integrating new technologies.

A full-time, funded Statewide Interoperability Coordinator also promotes efficiency and strengthens collaboration among statewide, regional, tribal, and national emergency communications entities. By increasing the number of full-time, funded Statewide Interoperability Coordinators, states are protecting responders and their ability to stay operable and interoperable during emergencies. The National Council of Statewide Interoperability Coordinators offers resources on its website to further educate states leadership on the Statewide Interoperable Coordinator's value.

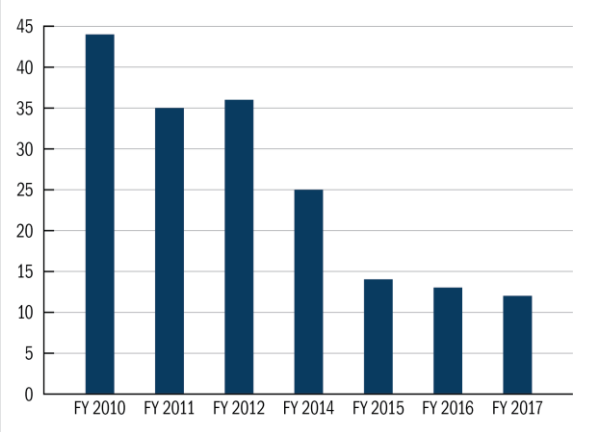


Figure 4: Decline in Full-time Statewide Interoperability Coordinators from 2010 to 2017

For instance, the Statewide Interoperability Coordinator plans and executes the statewide interoperability program, guided by stakeholder-driven initiatives in the NECP and the Statewide Communication Interoperability Plan and implemented by Tactical Interoperability Communications Plans. As such, Statewide Interoperability Coordinators act as linchpins establishing and maintaining emergency communications governance and planning across each state or territory by bringing together stakeholders from a broad spectrum of public safety communications systems and services. Federal departments and agencies and tribes would benefit from having a similar coordination point unifying interoperability policies, decisions, and processes scattered across its bureaus, components, offices, and programs.

The following are indicators of success for this objective.

Success Indicators

- ✓ *States and territories create or revise policy and plans to formalize and fund emergency communications governance bodies, such as Statewide Interoperability Governing Bodies*
- ✓ *Governance bodies develop and implement governing documents, such as charters or bylaws, to clarify roles, purpose, authority, and methods for adapting to change*
- ✓ *States and territories provide funding, authority, and governance to support a full-time Statewide Interoperability Coordinator in each state or territory, such as through the development of legislative language and mandates*
- ✓ *State and territory governance bodies prioritize communications needs and coordinate with the Statewide Interoperability Coordinator and other state-level planners on applications for federal financial assistance*
- ✓ *Federal departments or agencies establish a federal interoperability office or designate a Federal Interoperability Coordinator*

Supporting State 911 Administrators

The State 911 Administrator coordinates the operation of a state or territory's 911 system, as determined by state legislation or regulation. While the official title and role of this position may vary, the establishment of a state-level entity with authority to address essential 911 functions and responsibilities, is highly advantageous to maximizing the effectiveness and financial efficiency of statewide 911 systems. The State 911 Administrator interacts with originating telecommunications services and emergency responders, as well as facilitates operational functions for a statewide 911 system of systems.

As of December 2018, 45 states have State 911 Administrators, and the National Association of State 911 Administrators offers resources to educate leadership on the value of the State 911 Administrator.

Objective 1.2. Structure more inclusive governance by expanding membership composition

Governance benefits from including a variety of traditional and non-traditional entities supporting public safety, such as tribes, medical facilities, alerting authorities, nongovernmental organizations, public works, utilities, forestry services, military, private sector, and the American Red Cross. Coordination and planning through governance with these under-represented organizations or sectors will assist with the development of strategic, operational, and contingency plans.

The Nation is experiencing unprecedented changes in system connectivity, the types of technologies used, and the flow and potential exposure of data. Information technology officers (e.g., chief information officers) provide technical expertise on these issues, and their participation on governance subcommittees related to new technologies will assist with coordinating the integration of advanced technologies. Participation of elected officials and decision makers allows those making fiscal and policy decisions to better understand emergency communications requirements and priorities, empowering them to take informed action. Formal collaboration provides greater access to and understanding of strategic plans and short- and long-term priorities, as well as the ability to contribute to the formation of solutions and necessary support for key priorities and challenges at state, local, tribal, and territorial levels. The following are indicators of success for this objective.

Success Indicators

- ✓ *Governance bodies identify and include missing or underrepresented stakeholders (e.g., jurisdictions, tribes, sectors, and organizations) in formal governance structures, when developing strategic and operational plans and policies, during training and exercises*
- ✓ *Governance bodies include information management, network infrastructure, and cybersecurity representatives through membership or formalized coordination*
- ✓ *Governance bodies coordinate with elected officials to champion public safety communications priorities and lifecycle planning among decision makers*
- ✓ *Governance bodies coordinate and consult with tribal points of contact to develop cooperative strategies for achieving interoperability*

Tribal Resources for Coordination

Developing collaborative and trusted relationships among tribes and other governments is key to improving operable and interoperable communications. Strategies for working with tribes and tribal governance are as diverse as the number of tribes themselves. In 2018, there were 573 federally recognized sovereign tribal nations in the United States, most of which cross multiple states, counties, jurisdictions, and even countries. The 2018 update to the "Emergency Communications Governance Guide for State, Local, Territory, and Tribal Officials" highlights the crucial need to include tribes in planning and coordination processes. Recommendations from the Governance Guide strongly encourage representation and coordination with surrounding tribal nations on improving operable and interoperable communications with local, regional, and state governments.

Objective 1.3. Adopt adaptive governance strategies to address the rapid evolution of technologies, capabilities, and risks

Adaptive governance models are flexible and support collaborative decision making to build resilience in response to new Ecosystem challenges. This approach considers not only adjustments to stakeholder participation and integrated planning, but governance processes and arrangements that promote the investment of time and resources toward innovation and cross-organizational learning. In the context of emergency communications, public safety organizations should embrace initiatives promoting innovation and technology integration such as information sharing, smart spectrum optimization, and risk mitigation (e.g., cyber attacks and interoperability) within policies, regulations, and funding for security initiatives.

Adaptive governance regularly considers the entities involved in emergency communications (social), the creation and adoption of communications innovations (technology), changes to policies and laws affecting the public safety communications community (political), and shifts in grant funding requiring the need to identify alternative resources (economic). Adaptive governance models may also consider a phased approach to strategic planning, including forecasting needs in the short-, mid-, and long-term to convey the value of investments to heads of municipalities, town managers, city councils, and other officials. The following are indicators of success for this objective.

Success Indicators

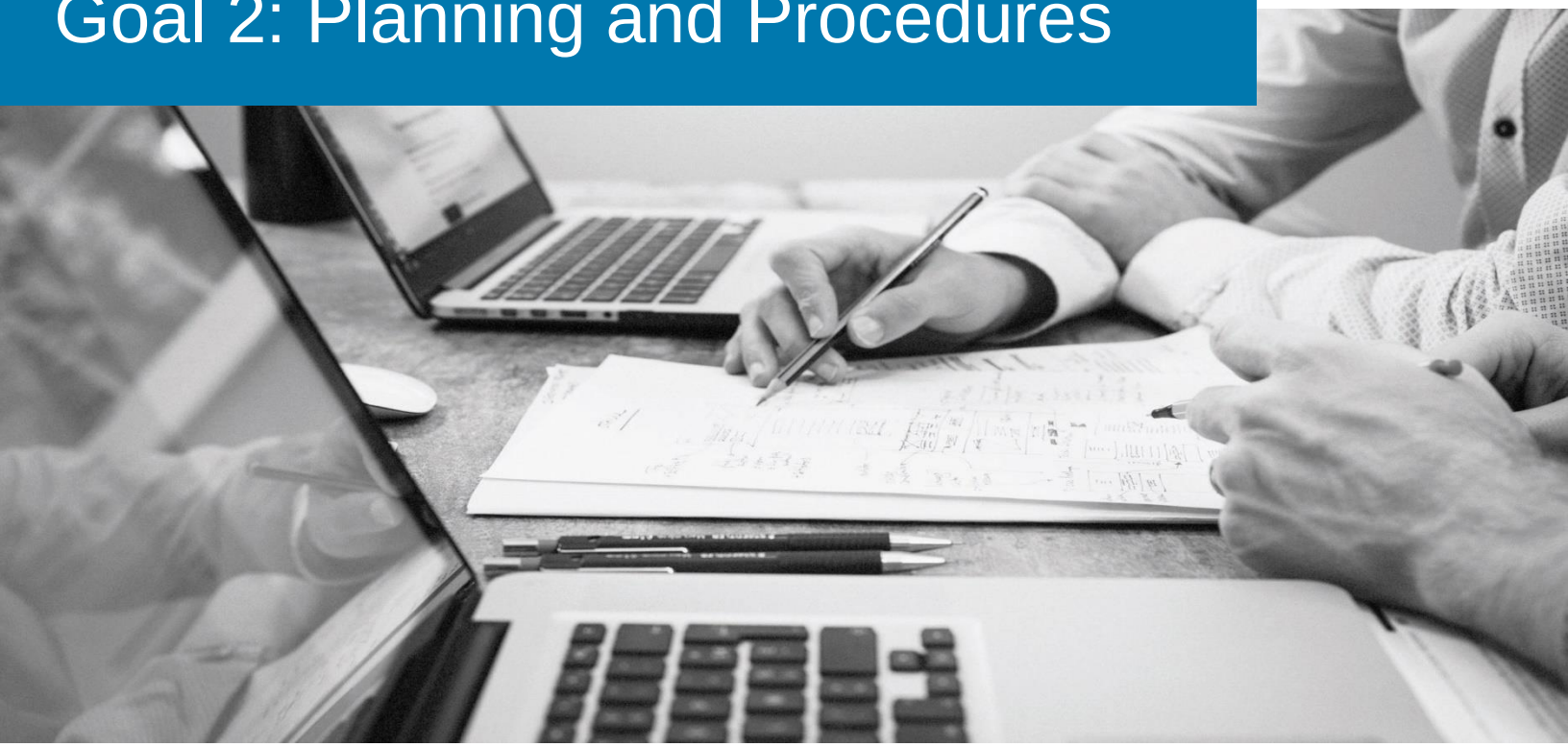
- ✓ *Governance bodies undertake technology integration and migration initiatives (e.g., broadband, 911, alerts and warnings, information management, network infrastructure, and cybersecurity) to guide implementation by public safety*
- ✓ *Governance bodies identify and address legislative and regulatory issues associated with emerging technology*
- ✓ *Organizations that support public safety communications formalize and regularly review cross-jurisdictional, multi-state, or multi-organizational agreements (e.g., memoranda of understanding, memoranda of agreement, and mutual aid agreements) to account for changes to resources, capabilities, and information- or technology-sharing needs*

- ✓ *The Emergency Communications Preparedness Center serves as a decision-making body guiding lessons learned, best practices, and partnerships for federal organizations implementing new capabilities*

Adapting Foundational Governance Practices:
2018 SAFECOM and National Council of Statewide Interoperability Coordinators Governance Guides

In 2018, SAFECOM and the National Council of Statewide Interoperability Coordinators updated the Emergency Communications Governance Guide for State, Local, Tribal, and Territorial Officials and the Emergency Communications Governance Guide for Federal Officials to enhance usability and applicability to a wider audience. The 2018 guides emphasize four key governance elements for adopting adaptive governance models, including (1) best practices for resource coordination, (2) funding and sustaining interoperability, (3) partnership formation, and (4) improving collaboration.

Goal 2: Planning and Procedures



Develop and update comprehensive emergency communications plans and procedures that address the evolution of risks, capabilities, and technologies across the Emergency Communications Ecosystem

Objective 2.1: Develop and regularly update strategic plans to align with the NECP and address the integration of new emergency communications capabilities (e.g., voice, video, and data)

Objective 2.2: Align emergency communications funding and investments with strategic and lifecycle planning

Objective 2.3: Incorporate risk management strategies to protect against and mitigate disruptions to mission-critical communications

Goal 2: Planning and Procedures

With the appropriate governance in place, formal written strategies, plans, and procedures guide the deployment of resources and technologies to achieve interoperable communications. Organizations increase their effectiveness by routinely updating these documents to evaluate the long-term direction of formal emergency communications guidance, including forecasting and gaining support for funding requirements through robust lifecycle planning. Rapid technological change requires a frequent reexamination of guidance that provide strategies to address the evolution of risks.

Objective 2.1. Develop and regularly update strategic plans to align with the NECP and address the integration of new emergency communications capabilities (e.g., voice, video, and data)

Given the rapidly evolving emergency communications and information technology environment, public safety organizations improve voice, video, and data interoperability and information exchange by planning for new investments, maintaining and modernizing legacy systems, and identifying the personnel and training needs that are necessary to meet new challenges. Strategic plans and roadmaps enable an organization to document its vision for the benefit of staff and partner agencies to prioritize communications resources, strengthen governance structures, identify future communications investments, and resolve long-standing operability and interoperability issues. Effective strategic plans consider multi-jurisdictional needs, standardization of technology interfaces specific to one's community and with surrounding jurisdictions, and processes for testing and updating plan milestones at all levels of government. Additionally, strategic planning for data interoperability incorporates (1) new partners (e.g., private and health sectors), (2) legal and policy aspects of information and data sharing, (3) funding support for integration and interface, (4) security concerns and solutions, and (5) preparations for forward compatibility of evolving technologies.

The primary emergency communications strategy for each state or territory is their Statewide Communication Interoperability Plan, which defines critical emergency communications capabilities and needs. States and territories work with their Statewide Interoperability Coordinator to align investments with their Statewide Communication Interoperability Plan and associated implementation plans to improve communications. Many federal emergency communications grants require recipients to align their projects to the Statewide Communication Interoperability Plan. As a result, state, local, tribal, and territorial public safety agencies benefit from contributing to the development or revision to plan content. The Emergency Communications Preparedness Center works with personnel at federal departments and agencies to ensure they have the tools needed to develop, coordinate, and share unique strategic plans across the interagency community to identify opportunities for cooperation. The following are indicators of success for this objective.

Success Indicators

- ✓ *Public safety organizations use strategic implementation plans (e.g., Statewide Communication Interoperability Plans, Regional Interoperability Communications Plans, Next Generation 911 Plans, and cybersecurity plans) to measure progress against NECP objectives and any additional state or territory objectives, and update plans annually*
- ✓ *Federal departments and agencies develop emergency communications strategic plans in coordination with the Emergency Communications Preparedness Center*

Objective 2.2. Align emergency communications funding and investments with strategic and lifecycle planning

Public safety organizations rely on complex and often expensive systems to carry out their missions. According to the 2018 Nationwide Communications Baseline Assessment, most public safety organizations have either no funding or insufficient funding for capital investments in interoperability solutions, interoperability-related operations, or maintenance costs. At the agency level, shortfalls in funding continue to affect the ability to properly maintain systems, conduct overall system lifecycle planning, and make decisions. Lifecycle planning requires public safety organizations at all levels of government to collaboratively and regularly assess needs, hazards, risks, and threats in the current environment and through the expected technology evolution. Consideration of short- and long-term technology evolution enables an organization to determine system needs and requirements as part of the lifecycle planning process. Identification of funding mechanisms to support those needs and requirements is a key component of lifecycle planning, as costs can be a determining factor in the replacement or refreshment of systems.

SAFECOM has produced a vast catalog of resources through its Funding and Sustainment Committee, including the annual SAFECOM Guidance on Emergency Communications Grants, which provides recommendations to grant applicants seeking federal funding. Additional resources are available on the SAFECOM Funding website, including guidance for lifecycle planning and identifying funding solutions. Public safety agencies seeking to effectively manage the ongoing investments necessary for systems and equipment may refer to the 2018 SAFECOM and the National Council of Statewide Interoperability Coordinators Emergency Communications System Lifecycle Planning Guide for recommendations, checklists, and suggested timelines. Public safety increasingly understands the need to diversify funding mechanisms and resources in its efforts to prioritize system sustainment and upgrade, as detailed in the SAFECOM and the National Council of Statewide Interoperability Coordinators Funding Mechanisms for Public Safety Communications Systems. This resource lists real-world examples for other agencies to consider. The following are indicators of success for this objective.

Success Indicators

- ✓ *Federal funding authorities develop grant guidance for emergency communications governance and investments consistent with guidelines provided by SAFECOM and the NECP*
- ✓ *Public safety organizations develop and use lifecycle plans to inform agency funding decisions and implement new technologies while maintaining necessary legacy and backup systems*
- ✓ *Public safety organizations and governing bodies identify sustainable funding mechanisms to support the lifecycle planning model*

Objective 2.3. Incorporate risk management strategies to protect against and mitigate disruptions to mission-critical communications

The modernization of emergency communications systems (e.g., Internet of Things, data interoperability, social media, and encryption) brings a wealth of new capabilities, as well as associated risks (e.g., system failures, cyber attacks, and data breaches). The DHS Threat and Hazard Identification and Risk Assessment and the Stakeholder Preparedness Review are helpful when conducting state-level capability evaluations. Communities participate in these interconnected processes to evaluate preparedness, including capabilities for emergency communications. State and local decision makers and Statewide Interoperability Coordinators should apply information within these assessments to direct funding and sustainment resources to new and legacy emergency communications systems.

Determining and testing strategies to increase the resiliency of public safety networks and the knowledge of personnel who administer them also helps to prevent catastrophic loss of critical communications during emergencies or disasters. Less than half of public safety organizations build processes into their plans to ensure continuity during out-of-the-ordinary emergencies or disasters (Figure 5). Incident response teams, incident response plans, recovery or resiliency plans, and continuity of operations plans are useful in cybersecurity incident response. Public safety organizations should review or develop continuity of operations plans and consider communications operability, interoperability, resiliency and security with respect to third-party service level agreements and interconnection providers. Information technology administrators may consider establishing a Computer Security Incident Response team or reach an agreement with CISA's Incident Response Team. Additionally, coordinating response and recovery efforts with the Statewide Interoperability Coordinators and other information technology administrators can increase cybersecurity posture. The following are indicators of success for this objective.

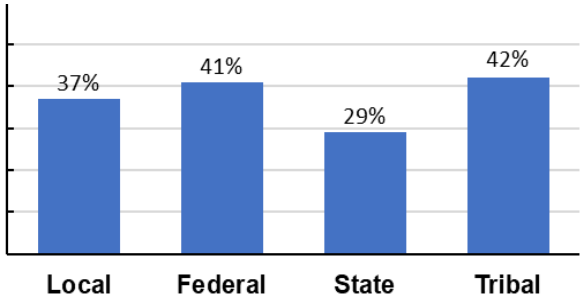


Figure 5: Percentage of Public Safety Organizations Whose Strategic Planning Process Does Not Ensure Continuity in Out-of-the-Ordinary Situations

Success Indicators

- ✓ *Local public safety organizations work with state agencies to evaluate emergency communications threats, hazards, and needs in formal capability reporting mechanisms (e.g., Threat and Hazard Identification and Risk Assessment and Stakeholder Preparedness Review)*
- ✓ *Public safety organizations incorporate risk management strategies into plans for continuity and recovery of critical communications*
- ✓ *Public safety organizations that use information technology have a cybersecurity incident response plan in place*
- ✓ *Public safety organizations perform resiliency assessments and mitigate vulnerabilities*

Goal 3: Training, Exercises, and Evaluation

Develop and deliver training, exercise, and evaluation programs that enhance knowledge and target gaps in all available emergency communications technologies

Objective 3.1: Update and ensure the availability of training and exercise programs to address gaps in emergency communications

Objective 3.2: Incorporate human factors in training and exercises to address the demands that voice, video, and data information place on personnel

Objective 3.3: Ensure training addresses information sharing (e.g., voice, video, and data) for multi-agency responses

Goal 3: Training, Exercises, and Evaluation

Effective training and exercise programs bolster emergency professionals' proficiency with communications equipment, as well as improve their ability to execute policies, plans, and procedures governing the use of communications. The 2018 Nationwide Communications Baseline Assessment findings reflect strong participation in training and exercise programs, indicating progress in the right direction. However, as new and emerging technologies are introduced, it is vital for training and exercise programs to evolve as well. Allowing personnel to routinely practice with new communications capabilities maximizes the benefits and use during an incident. It is important for the public safety community to support communications-specific training and exercise programs, proper evaluation to identify and close gaps, expansion of regular training and exercises through increased awareness and augmentation of available opportunities, and more aggressive tracking and use of National Incident Management System Incident Command System-capable communications support personnel.

Objective 3.1. Update and ensure the availability of training and exercise programs to address gaps in emergency communications

While the public safety community has made progress, there remains a need to update and implement training and exercise programs to address gaps and ensure personnel are proficient in the increasing number of diverse capabilities used during incident response. As depicted in Figure 6, the 2018 Nationwide Communications Baseline Assessment findings reflect strong participation in training and exercise programs overall. However, more than a quarter of local public safety organizations and almost one-third of federal and tribal organizations do not participate in exercises. These results indicate opportunities to expand training and exercise participation and content to address new technologies, threats, and organization-specific planning needs. Communications-focused training and exercises demonstrate and test interoperability and continuity capabilities during unplanned incidents. Effective training and exercise programs also incorporate changes in policies, standard operating procedures, partners, and technologies as they occur.

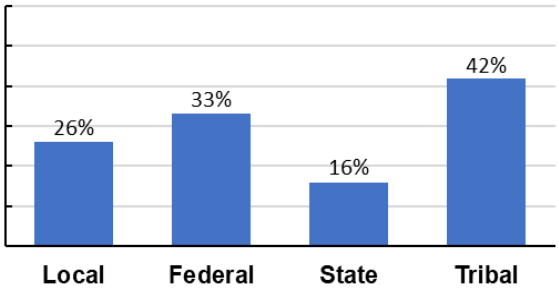


Figure 6: Percentage of Public Safety Organizations That Do Not Participate in Exercises

By assessing communications during exercises and real-world events and incidents, public safety organizations can improve operational procedures, policies, and training program effectiveness. Public safety captures improvement-related data through a repetitive, periodic analysis of tabletop, functional, and full-scale exercises; planned events; and incident after-action reports. Outcome-focused documentation identifies points of system failure, coverage inadequacies (indoor and outdoor), and requirements for primary, secondary, and backup systems. Deficiencies and unmet needs form the basis of an organization's improvement action plan, which presents solutions to strengthen communications coordination.

The Homeland Security Exercise and Evaluation Program is the national standard for developing exercises with objectives supported by exercise evaluation guidelines. The public safety community can enhance emergency communications through the evaluation of training and exercises by using communications support personnel in federally funded exercises and third-party or peer evaluations.

Training Videos for DHS Priority Telecommunications Services

DHS has a series of technical how-to training videos covering many aspects of the Government Emergency Telecommunications Service, Wireless Priority Service, and Telecommunications Service Priority, as well as a half-hour video webinar on all three programs. The how-to videos run approximately 3 to 4 minutes each and cover the following:

- How to Enroll in Government Emergency Telecommunications Service, Wireless Priority Service, and Telecommunications Service Priority
- How to Make a Government Emergency Telecommunications Service Call
- How to Make a Wireless Priority Service Call
- What to Do When the Government Emergency Telecommunications Service Access Number Doesn't Work
- Programming Government Emergency Telecommunications Service / Wireless Priority Service into your Phone Contacts List
- How to Request Provisioning or Restoration Once Enrolled in Telecommunications Service Priority

The videos and webinar are available at http://www.cisa.gov/pts-videos.

Evaluations are only effective if training and exercise programs are improved through incorporation of lessons learned. However, the 2018 Nationwide Communications Baseline Assessment found most public safety organizations do not document or assess training evaluations along with the changing operational environment. The following are indicators of success for this objective.

Success Indicators

- ✓ *Public safety organizations develop or update training and exercise programs to address new technologies, data interoperability, cybersecurity, use of federal and national interoperability channels, personally identifiable information, and continuity of communications*
- ✓ *Public safety personnel across multiple agencies and jurisdictions are registered for communications training classes and exercises whenever possible*
- ✓ *Public safety organizations coordinate training and technical assistance across levels of government (as applicable) to ensure current and consistent information*
- ✓ *Public safety organizations include injects in exercises to test communications systems and personnel (including emerging technology and system failure) and utilize third-party evaluators with communications expertise*
- ✓ *Public safety organizations integrate private sector, nongovernmental organizations, and public sector communications stakeholders into training and exercises*
- ✓ *The Emergency Communications Preparedness Center analyzes gaps and identifies opportunities for federal interagency training and exercise programs*

Objective 3.2. Incorporate human factors in training and exercises to address the demands that voice, video, and data information place on personnel

Training resources must keep pace with the integration of new communications technologies and services made available to public safety professionals. More technologies and applications result in more data to process, more standard operating procedures to learn, and more stress for the users. To ensure effective use of all available technologies when a responder is under duress, progressive training and exercise programs can be designed to build on previous lessons and add new objectives along the way. Progressive training and exercises not only build upon each other, but increased repetition develops "muscle memory," leading to the likelihood that public safety professionals will use available technologies appropriately and effectively during incidents and planned events.

In the field, new technologies such as body-worn cameras are changing the nature of incident responses and require training to be used effectively. New technologies bring responders not on-scene closer to the impacts of a threat or hazard through photos, videos, and live streaming. One downside to repetitive training is that repeated exposure to graphic incident scene images can increase the risk of post-traumatic stress in responders. Public safety agencies will benefit from incorporating modules demonstrating techniques to combat compassion fatigue or vicarious trauma into trainings and building opportunities to practice those methods into exercises. The following are indicators of success for this objective.

Success Indicators

- ✓ *Public safety organizations implementing mobile data applications utilize training and tools to ensure that responders effectively use and are not overloaded by available information*
- ✓ *Public safety organizations implement tools and trainings to address emerging technology impacts*

Objective 3.3. Ensure training addresses information sharing (e.g., voice, video, and data) for multi-agency responses

DHS has trained more than 7,000 all-hazards communications support personnel nationwide, resulting in a significant pool of trained staff in every state and territory. While a cadre of thousands of Communications Unit Leaders and Communications Technicians have been trained, agency leadership often does not know or take advantage of this capability during actual responses. Accessing these resources is difficult when some states do not have a program with policies and procedures to track, maintain, and use National Incident Management System Incident Command System-capable communications support resources. The NECP promotes progress for Emergency Support Function #2 and Communications Unit positions to more effectively integrate personnel into operations and to improve capabilities to track and share trained communications-support personnel.

The ongoing training and development of communications-support personnel is an essential part of public safety response to planned events and unplanned incidents, particularly as the scope and complexity of technologies evolve. In 2018, DHS began developing a course for the Information Technology Service Unit Leader to address increased demand for information technology devices and networks during an incident or planned event. The Information Technology Service Unit Leader course ensures that communications-support resources are equipped with adequate skills to operate and troubleshoot information equipment during an activation and to enable service improvements over time. Advances in tracking the training and use of active communications-support personnel resolve shortages during an incident or event and fulfill federal, state, local, tribal, and territory requirements for these positions. The following are indicators of success for this objective.

Success Indicators

- ✓ *States, territories, and tribal nations implement programs (based on best practices) to oversee the qualification, training, certification, recognition, activation, and currency of communications-support personnel*
- ✓ *States, territories, and tribal nations develop and support instructor cadres to expand training for communications-support personnel*
- ✓ *SAFECOM and the National Council of Statewide Interoperability Coordinators develop training curriculums for additional positions within the Information Technology Service Unit*

Communications Unit Personnel Position Task Book Sign-Off Process Template

As defined by the National Incident Management System Incident Command System, Communications Unit personnel plan and manage the technical and operational aspects of the communications function during an incident or event. To obtain a Communications Unit, Communications Unit Leaders, or Communications Technicians status, trainees must complete a Position Task Book documenting their ability to perform the functions required of a Communications Unit position. The National Council of Statewide Interoperability Coordinators Planning, Training, and Exercise Committee, in conjunction with the SAFECOM Communications Section Task Force, developed a Position Task Book Sign-Off Process Template to assist Statewide Interoperability Coordinators, Statewide Interoperability Coordinator designees, state governance bodies, and regional governance bodies in developing a system for Communications Unit Personnel Position Task Book sign-off.

Goal 4: Communications Coordination

Improve effective coordination of available operable and interoperable public safety communications capabilities for incidents and planned events

Objective 4.1: Confirm the implementation of the National Incident Management System

Objective 4.2: Enhance coordination and effective usage of public safety communications resources at all levels of government

Objective 4.3: Develop or update operational protocols and procedures to support interoperability across new technologies

Objective 4.4: Strengthen resilience and continuity of communications throughout operations

Goal 4: Communications Coordination

Effective coordination and efficient usage of all available communications capabilities are critical to ensuring both responder safety and the timely provision of public safety services. Familiarity with the operation of existing technologies prior to an incident response minimizes communications challenges. Similarly, the advantages of new technologies can only be maximized when familiarity and usage of the capability comes in the form of repeated real-world application of the technology during operations. While exercise, event, and incident after-action reports reflect improvements in coordination using communications technologies, challenges remain due to continuous technological advancements.

The significant benefits that communications technologies may introduce to the coordination of incidents and planned events are lost if not applied appropriately. New, improved, or updated features, functions, and capabilities must be accounted for in policies, plans, and procedures. The introduction of new and improved technologies and additional communications capabilities can make coordination more complex and challenging until their usage is more commonplace across the entire spectrum of public safety users. Nevertheless, public safety organizations enhance coordination when they proactively incorporate new and improved communications technologies, as well as engage commercial and non-traditional communications systems providers.

Objective 4.1. Confirm the implementation of the National Incident Management System

Public safety organizations use the National Incident Management System Incident Command System processes, methods, and structures across all disciplines, jurisdictions, and levels of government to standardize methods, practices, and actions during planned events and incident responses. As public safety organizations maintain, implement, upgrade, or replace existing communications capabilities, those capabilities should reflect an alignment with the National Incident Management System Incident Command System doctrine to ensure available fielded capabilities are sufficient to support primary, secondary, and backup services. Depending on the incident size, scope, location, and progress, various resources may be pressed into service to support an evolving incident. The Incident Commander or Incident Management Team remains informed about the status of all available operable and interoperable communications capabilities through sharing appropriate Incident Command System form(s).

Public safety organizations are experiencing increased information sharing from various sources when larger complements of communications resources are deployed during initial responses to incidents. These heightened responses require pre-planning among public safety organizations, Incident Commander and Incident Management Team personnel, and communications systems providers. Coordination with communications systems providers helps to improve responders' awareness of expected timelines for incident response. The result is coordinated, robust, flexible, and resilient voice and data communications capabilities to effectively support incident objectives. The following are indicators of success for this objective.

Success Indicators

- ✓ *Public safety organizations possess primary, secondary, and backup communications capabilities aligned with the National Incident Management System Incident Command System and share appropriate forms (e.g., Incident Command System 205) illustrating the status of an agency's capabilities*

- ✓ *Public safety organizations assess and improve the timeliness of notification, activation, and response of communications systems providers to support the Incident Commander and Incident Management Team requirements at incidents and planned events*

Objective 4.2. Enhance coordination and effective usage of public safety communications resources at all levels of government

As the complexity of communications systems increases at a significant pace, it is incumbent upon public safety organizations to include their communications systems providers in planning and response activities. These resources offer technical assistance and advice to improve coordination for planned events and incident responses. Communications systems providers may be internal, external, or a combination of both, and their expertise, knowledge, and access to additional communications resources can be the difference between successful or failed incident responses. Public safety organizations should evaluate existing communications policy, plans, agreements, and current systems and capabilities usage to determine appropriate inclusion of commercial providers and non-traditional communications partners.

Knowledge of the availability and state of all interoperable communications assets is essential to coordination efforts. At a minimum, public safety organizations need to share current communications systems information with contiguous public safety agencies and other organizations that provide or receive mutual aid, share infrastructure, or participate in planned events. Sharing active, available features, functionality, and capabilities of communications resources with partners can expedite communications coordination for both incidents and planned events. The following are indicators of success for this objective.

Success Indicators

- ✓ *Public safety organizations maintain and readily share comprehensive information about features, functionality, and capabilities of operable and interoperable communication resources*
- ✓ *Public safety organizations use up-to-date defined practices, procedures, pre-plans, specific venue/location response plans, incident type response plans, standard operating procedures, tactical response directives, and/or Tactical Interoperability Communications Plans that identify primary, secondary, and backup communications assets (e.g., networks, devices, and applications) for effective communications coordination and information sharing during planned events and incidents*
- ✓ *Public safety organizations periodically evaluate, engage, and incorporate commercial and non-traditional communications partners (e.g., auxiliary communications, volunteers, and utilities) in incidents and planned events*
- ✓ *The state-level alerting authority and relevant lower-level alerting authorities ensure the highest state of readiness of existing capabilities for resilient and interoperable alerts, warnings, messaging and notifications using current local, county, state, and federal systems, and, when applicable, the Integrated Public Alert and Warning System (IPAWS)*

Objective 4.3. Develop or update operational protocols and procedures to support interoperability across new technologies

As of 2018, a significant number (almost 25 percent) of public safety agencies lacked standard operating procedures for emergency communications. However, the fast-paced evolution of communications capabilities highlights a crucial need to develop and update standard operating procedures and operational plans to address entities, individuals, or organizations that provide or use communications during emergencies (e.g., utilities, transportation sector, and commercial carriers). Coupled with effective planning, training, and exercises, standard operating procedures transform policies and best practices into real-world operational plans, which detail how to establish and maintain communications during an incident or disaster. Analyzing after-action reports following events can assist with resolving gaps or missing information through the development or revision of standard operating procedures.

SAFECOM Standard Operating Procedures Resources

Visit the SAFECOM website to learn more about how to develop policies for coordinating interoperability during incident response, including tips for communities developing standard operating procedures, such as written guidelines for the use of intra-jurisdictional interoperability channels.

Public safety organizations should establish and maintain a repeatable process to periodically observe and record user proficiency for primary, secondary, and backup communications systems. This includes the ability of end-users to properly access, navigate, manipulate, and use the available features, functions, and capabilities of their communications devices and equipment. Observations that illustrate a lack of proficiency in the use of communications capabilities, established by sets of minimum standards, should drive recommendations for the modification of documentation, training, and exercises. The following are indicators of success for this objective.

Success Indicators

- ✓ *Public safety organizations develop and regularly update National Incident Management System-aligned standard operating procedures to facilitate the integration, deployment, and use of communications assets*
- ✓ *Public safety organizations have recommended guidelines regarding the use of personal devices (e.g., bring your own device) based on applicable laws and regulations*
- ✓ *Public safety organizations leverage training, exercises, and real-world events to test capabilities and update standard operating procedures*
- ✓ *Public safety organizations periodically review their use of Priority Telecommunications Services (e.g., Telecommunications Service Priority, Government Emergency Telecommunications Service, and Wireless Priority Service) and FirstNet, and ensure they have standard operating procedures governing the programs' use, execution, and testing*
- ✓ *Public safety organizations periodically assess the proficiency of personnel in using communications systems' features, functions, and capabilities*

Objective 4.4. Strengthen resilience and continuity of communications throughout operations

As emergency communications systems and functions become more interconnected, they also become more susceptible to physical and cyber vulnerabilities and disruptions in other parts of the Emergency Communications Ecosystem. Agencies at all levels of government must plan for the interconnection of voice and data communications. During large-scale events, planning and operations for backup communications need to include available assets and resources in the impacted incident area. For example, land mobile radio and cellular systems may need to be augmented by air, space, and marine mobile communications to create a comprehensive air, sea, and ground network with appropriate levels of security and authentication to ensure continuity of communications. Commercial cellular voice and data networks are often used as well. Regardless of the technology, any network may be overwhelmed by congestion or damage during an incident.

Achieving secure and resilient voice and data communications across the Ecosystem is essential for public safety agencies to execute their missions under any circumstances. To achieve this level of preparedness, public safety organizations and communications systems providers continually assess the readiness of currently available primary, secondary, and backup communications capabilities. Commonly, public safety communications capabilities are constructed, operated, and maintained to provide the highest levels of availability and access. The incorporation of resiliency and redundancy features ensures resources are available to effectively support critical communications for large numbers of emergency responders, while continuing to support other activities throughout a public safety organization's jurisdiction. The following are indicators of success for this objective.

Success Indicators

- ✓ *Public safety organizations establish sufficient testing and usage observations of all operable and interoperable primary, secondary, and backup communications systems*
- ✓ *Emergency communication centers/public safety answering points address systems and staffing to support communications continuity-of-operations planning*
- ✓ *SAFECOM and the National Council of Statewide Interoperability Coordinators develop best practices to encourage active network sharing and regionalization of shared services*

Shared System Project: Puerto Rico and the U.S. Virgin Islands

In the wake of the 2017 hurricane season, federal users in Puerto Rico and the U.S. Virgin Islands began collaborating on a single, actively shared federal land mobile radio communications network that can expand to include other technologies and subscribers. This shared systems project is a joint collaboration pilot led by CISA, U.S. Immigration and Customs Enforcement, and DHS Joint Wireless Program Management Office.

Goal 5: Technology and Infrastructure

Improve lifecycle management of the systems and equipment that enable emergency responders and public safety officials to share information efficiently and securely

Objective 5.1: Support public safety requirements that drive research, development, testing, and evaluation of emergency communications technology

Objective 5.2: Ensure communications and information sharing systems meet public safety's mission-critical needs

Objective 5.3: Support data interoperability through the development of effective and sustainable information sharing and data exchange standards, policies, and procedures

Goal 5: Technology and Infrastructure

The rapid rate of technology advancement continues to outpace the public safety community acquisition cycle. New technologies have the potential to be expensive and disrupt mission-critical operations. Yet, emerging technologies (e.g., wireless data networks, artificial intelligence, and mobile communications devices) offer advanced capabilities to enhance command and control and situational awareness for emergency responders. The ability to develop, test, and evaluate new technologies before integrating them ensures successful operability and interoperability with existing systems.

The public safety community has placed an emphasis on accelerating research, development, testing, evaluation, and standards implementation for emerging technologies that improve communications. With acknowledgement of the need for data capabilities, many public safety organizations have focused their technology efforts on preparing to implement broadband solutions. In addition, independent, statewide, and regional Project 25 radio systems and the foundation for Next Generation 911 systems are being deployed. The public safety community continues to develop strategies and technology roadmaps for implementing standards-based, vendor-neutral devices and applications that can sustain the unique public safety operating environment and provide mission-critical communications.

Objective 5.1. Support public safety requirements that drive research, development, testing, and evaluation of emergency communications technology

To improve the development of innovative emergency communications capabilities, public safety organizations must coordinate their approach to research, development, testing, and evaluation. There must also be action to accelerate the development and adoption of mission-critical, standards-based communications technology products, applications, and services. The following are indicators of success for this objective.

Success Indicators

- ✓ *SAFECOM and the National Council of Statewide Interoperability Coordinators identify public safety technology and infrastructure capability gaps*
- ✓ *The Emergency Communications Preparedness Center coordinates federal research, development, testing, and evaluation priorities and processes*
- ✓ *The Emergency Communications Preparedness Center cultivates sustained engagement (e.g., cooperative agreements) between federal research, development, testing, and evaluation programs (e.g., DHS's Science and Technology Directorate and the National Institute of Standards and Technology's Public Safety Communications Research Division) and public safety organizations to address resiliency, interoperability, and other challenges*
- ✓ *The Emergency Communications Preparedness Center partners with the private sector to foster an open, innovative, and standards-based commercial marketplace for solutions development and ensures that public safety requirements are addressed in current and emerging standards*

Objective 5.2. Ensure communications and information sharing systems meet public safety's mission-critical needs

Public safety organizations must continually evaluate and implement communications standards and programs to keep pace with technological advancements. Once a technology has been successfully tested and evaluated to meet public safety needs, standards must be developed or refined to ensure compatibility with existing systems and enable consistent implementations across the Emergency Communications Ecosystem. Programs that facilitate technology adoption are necessary to communicate benefits and minimize risk. New or enhanced technology may not be appropriate for every public safety organization's mission, nor can new or enhanced technology be adopted without consideration of impacts to governance, standard operating procedures, use, training, and exercises. The following are indicators of success for this objective.

Success Indicators

- ✓ *SAFECOM and the National Council of Statewide Interoperability Coordinators communicate emerging technology impacts to public safety, such as those associated with identity management, multimedia, 5G, Internet of Things, social media, network virtualization, spectrum optimization, artificial intelligence, machine intelligence, geographic information systems, and positioning, navigation, and timing systems*
- ✓ *SAFECOM and the National Council of Statewide Interoperability Coordinators guide standards-based land mobile radio evolution*
- ✓ *Public safety organizations support the development and implementation of resiliency standards and guidelines to protect against events such as natural disasters, network and grid failures, terrorism, lightning, and electromagnetic pulse events*
- ✓ *The FirstNet Authority innovates and integrates broadband technology into the Nation's public safety communications infrastructure*
- ✓ *The National 911 Program coordinates, in collaboration with all levels of government, the optimization of 911 services, including the Nation's transition to Next Generation 911*

Next Generation 911 Technology and Infrastructure Activities

- Convert all addressing to geographic information system.
- Establish dedicated Emergency Services Internet and Next Generation 911 Core Services.
- Install Next Generation 911-capable and standard-compliant 911 Customer Premises Equipment as well as Computer-Aided-Dispatch.
- Create a robust mechanism for integration of devices and applications through a technical review and acceptance process supported by commercial and public safety standards.
- Develop and rapidly adopt standards facilitating the interface between 911, Computer-Aided-Dispatch, and FirstNet
- Develop and rapidly adopt technical models to manage the receipt, processing, and sharing of multimedia.

FirstNet Technology and Infrastructure Activities

- Establish a dedicated (physically separate) Public Safety Long-Term Evolution Core.
- Deploy and expand a nationwide Radio Access Network with Band 14 coverage and capacity.
- Create a robust, device ecosystem through a technical review and acceptance process supported by commercial and public standards.
- Establish an application catalog and developer's portal for an open, integrated applications ecosystem, tailored to public safety users.
- Give access to 72 dedicated FirstNet Authority deployables plus access to hundreds of other long-term evolution deployables.
- Accelerate delivery of mission-critical long-term evolution services, such as mission-critical push-to-talk, mission-critical video, and mission-critical data.
- Focus resources in key technology areas (e.g., coverage and capacity, situational awareness, voice communications, secure information exchange, and user experience) to improve public safety operations.

Objective 5.3. Support data interoperability through the development of effective and sustainable information sharing and data exchange standards, policies, and procedures

Data sharing capabilities have continued to evolve, shaping the way information is communicated and shared. Emerging capabilities expand with whom and how agencies can share information before, during, and after an event. While the exchange of data can improve situational awareness and facilitate transfer of mission-critical information, the quickly evolving and complex culture of data sharing also brings risk and privacy considerations. Documented in the 2018 Nationwide Communications Baseline Assessment, on average, less than half of public safety organizations use or test interoperability solutions for data (Figure 7).

One challenge for effective information exchange is the increase in the types of data being exchanged. Common data types in the Ecosystem now include video, geographic information system data, evacuee/patient tracking data, accident/crash (telematics) data, biometric data, Computer-Aided Dispatch data, Automatic Vehicle Location data, Common Operation Picture data, and more.

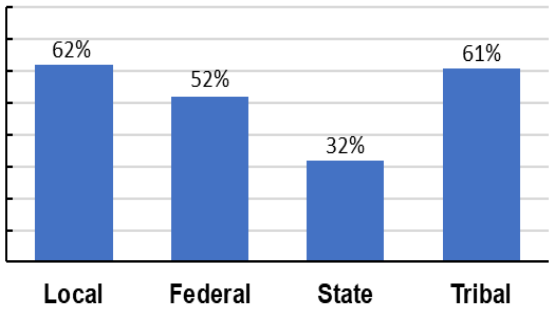


Figure 7: Percentage of Public Safety Organizations That Never Use or Test Interoperability Solutions for Data

Another challenge is the volume of data requiring storage, exchange, maintenance, and analysis. The development of effective and sustainable information exchange models and data sharing standards, policies, and procedures will help the public safety community address their data management needs, and enable them to adopt solutions for Big Data, Internet of Things, cloud convergence, and other data-intensive disruptive technologies. The following are indicators of success for this objective.

Success Indicators

- ✓ *Public safety organizations employ standards-based information exchange models and data sharing solutions*
- ✓ *Public safety organizations follow acquisition best practices, including consideration for standards-based infrastructure*
- ✓ *SAFECOM and the National Council of Statewide Interoperability Coordinators publish best practices and updated guidance on standard operating procedures to help the public safety community overcome data storage, exchange, maintenance, and analysis challenges*

Goal 6: Cybersecurity

Strengthen the cybersecurity posture of the Emergency Communications Ecosystem

Objective 6.1: Develop and maintain cybersecurity risk management

Objective 6.2: Mitigate cybersecurity vulnerabilities

Objective 6.3: Determine public safety-specific, standards-based cyber hygiene minimums and fund ongoing risk mitigation

Goal 6: Cybersecurity

To prepare for cyber incidents, the public safety community must continually identify risks and evolve security requirements in coordination with partners in their Emergency Communications Ecosystem. Cybersecurity is a shared mission across all levels of government, the private sector, nongovernmental organizations, and the public.

As noted in the 2017 National Preparedness Report, despite significant interest in and need for cybersecurity, most states and territories have low confidence in their cybersecurity capabilities. To address this need, the Federal Government established several programs to offer resources to help organizations manage their cybersecurity risk. For example, organizations can utilize self-assessment guides from DHS's Cyber Resilience Review program to uncover gaps and areas for improvement.

As cyber threats and vulnerabilities grow in complexity and sophistication, incidents become more numerous and severe against emergency communications systems. Therefore, it is critical that public safety organizations take proactive measures to carefully manage their cybersecurity risks.

Objective 6.1. Develop and maintain cybersecurity risk management

Establishing cybersecurity risk management can help organizations identify and prioritize risks, protect resources, detect threats, and enable coordinated, effective response and recovery. Despite every effort, cyberthreat events will occur. Figure 8 illustrates the significant percentages of public safety organizations affected by known cybersecurity breaches, according to results from the 2018 Nationwide Communications Baseline Assessment. Each organization should be prepared to execute response processes and procedures, prevent expansion of the event, and mitigate its effects. Incident response plans, recovery or resiliency plans, and continuity of operations plans are useful in a cybersecurity incident response. Recovery planning processes and strategies are improved by incorporating lessons learned into future activities. Response personnel should be trained on the latest security, resiliency, continuity, and operational practices and maintain in-service training as new technology and methods are made available. The following are indicators of success for this objective.

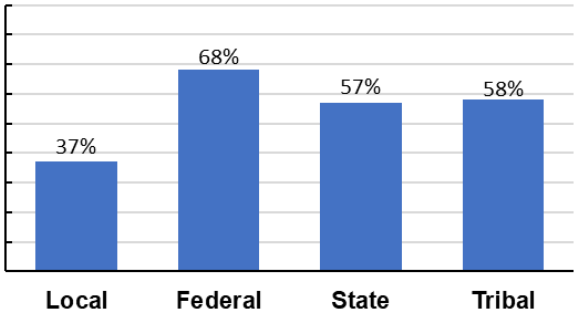


Figure 8: Percentage of Public Safety Organizations Whose Communications Have Been Impacted by Cybersecurity Breaches at Some Point in the Last 5 Years

Success Indicators

- ✓ *Public safety organizations, at a minimum, implement the National Institute of Standards and Technology Cybersecurity Framework*
- ✓ *Public safety organizations perform a Cyber Resilience Review*

Objective 6.2. Mitigate cybersecurity vulnerabilities

The identification and mitigation of threats and vulnerabilities is a shared responsibility. Threat information sharing and shared solution sets are important aspects of cybersecurity. Public safety organizations must make difficult decisions to allocate attention and funding to manage their cybersecurity risk. They must also consider the impacts of their cybersecurity risk management on interoperability with the broader community. For example, voice and data encryption is increasingly used throughout the public safety community to mitigate threats. Data encryption implementation is natively included in many applications and should be implemented when sensitive data might be transmitted. Some voice applications also natively include encryption, but in other technical and operational environments, it may be difficult and expensive to implement voice encryption. In these situations, the reduced cybersecurity risks of voice encryption may need to be compared against the potential increased complications and costs. Only when working together will the public safety community be able to implement the most cost-effective and efficient mitigation activities and approaches that enable them to maintain the highest degree of interoperability.

Encryption and Key Management Resources

For more guidance on encryption and key management, review the Best Practices for Public Safety Interoperable Communications.

SAFECOM and the National Council of Statewide Interoperability Coordinators continue to produce guidance educating the community on known mid- and long-term threats and their mitigations. In addition, SAFECOM and the National Council of Statewide Interoperability Coordinators maintain working groups (e.g., the Next Generation 911 Working Group) that focus on specific segments of the Ecosystem. Public safety organizations should also leverage the continual work performed by the National Institute of Standards and Technology and other standards-development organizations to review equipment and protocol vulnerabilities. The following are indicators of success for this objective.

Success Indicators

- ✓ *SAFECOM and the National Council of Statewide Interoperability Coordinators share planning and mitigation guidance regarding known threats and vulnerabilities*
- ✓ *SAFECOM and the National Council of Statewide Interoperability Coordinators encourage cybersecurity for Next Generation 911*
- ✓ *Public safety organizations leverage ongoing efforts by the National Institute of Standards and Technology and standard development organizations to identify and mitigate equipment and protocol vulnerabilities that impact the public safety mission*

Objective 6.3. Determine public safety-specific, standards-based cyber hygiene minimums and fund ongoing risk mitigation

Instituting a "security first" perspective for public safety requires stakeholders to join together and establish consistent standards, policies, procedures, interoperability, and implementation guidance for emergency communications deployments, including consideration of the significant costs of these activities. The 2018 Nationwide Communications Baseline Assessment revealed a significant percentage of public safety organizations lack the funding to address their cybersecurity needs (Figure 9).

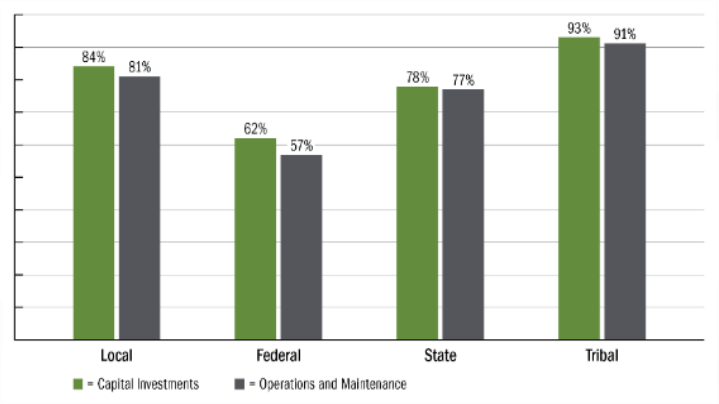


Figure 9: Percentage of Public Safety Organizations That Have No Funding or Insufficient Funding to Meet Cybersecurity Needs

Cybersecurity is a continual process of enhancing defense. Therefore, public safety should leverage ongoing National Institute of Standards and Technology work to plan for setting, testing, and maintaining cyber minimum standards to assist cybersecurity-eligible grant programs in prioritizing and distributing necessary funding to public safety. To promote the importance of cybersecurity, it should be included as a critical success element in the SAFECOM Interoperability Continuum, which assists emergency response organizations and policymakers to plan and implement interoperability solutions for data and voice communications. National programs and federal agencies also have a role in evaluating, communicating, and advocating for cybersecurity services and resources. The following are indicators of success for this objective.

Success Indicators

- ✓ *The National Institute of Standards and Technology's Public Safety Communications Research Division establishes recommended public safety-specific, standards-based cyber hygiene minimums for public safety*
- ✓ *SAFECOM updates the Interoperability Continuum to account for cybersecurity*
- ✓ *SAFECOM and the National Council of Statewide Interoperability Coordinators consolidate and publish information on cybersecurity services and grant programs, such as those detailed in the DHS Cybersecurity Services Catalog and the Homeland Security Grant Program*
- ✓ *CISA studies the cost of cyber incidents in support of cybersecurity risk management*
- ✓ *The National Institute of Standards and Technology's Public Safety Communications Research Division provides incentives for public safety-specific, cybersecurity-specific research and development activities based on known threats*

Implementing the NECP

The NECP goals and objectives provide the blueprint to enhance emergency communications capabilities nationwide, consistent with legislative requirements. DHS has a practiced strategy for implementing, measuring, and reporting progress on the NECP in coordination with stakeholders, working together toward the desired end-state of emergency communications.

Implementation Action Plan and Promotion

CISA is designated as the federal agent charged with overseeing NECP implementation. In this role, the agency will use a two-step approach for implementation: (1) develop and execute an action plan that supports the NECP's six goals and supporting objectives; and (2) develop and execute a nationwide publication campaign to promote the NECP. Both steps will be coordinated in partnership with stakeholders from the public safety community.

Although CISA leads the development and management of the NECP, the implementation is a shared responsibility among DHS and the plan's stakeholders. This reflects the nature of the public safety community, which spans disciplines, jurisdictions, and levels of government, and involves the public and private sectors. As such, the action plan will identify supporting activities that CISA programs, services, or offerings can update or modify, develop, and enact to implement the NECP. It will further coordinate with federal, state, local, tribal, and territorial agencies to identify actions each can take to further support the plan's implementation activities. CISA will also work with stakeholders to plan actions within the constraints of limited resources, as the NECP does not directly provide funding to implement.

The NECP is published on the DHS website and recognized as the strategic plan for the Nation. Similar to past releases, CISA will launch a promotional campaign following publication to drive the whole community toward its desired end-state as described in the NECP vision. CISA will enlist its Regional Coordinator personnel and champions from federal, state, tribal, territorial, regional, jurisdictional, and local agencies to promote NECP implementation through stakeholder engagements and public safety associations. The plan's success relies on the whole community embracing the NECP goals and objectives, and most importantly acting on them.

Measuring Progress

The ability of responders to seamlessly communicate and share information to save lives and protect property is both the most important and challenging criteria by which to measure the NECP's success. Given the multitude of public safety agencies across the Nation, and the large number of incidents to which they respond to daily, a consistent evaluation of how well communications function during response operations is a major challenge that requires cooperation at all levels of government.

To assess progress in achieving the NECP goals and objectives, CISA will use the following approach:

- Coordinate with the public safety community to share goals and objectives to incorporate them into emergency communications plans.
- Use the success indicators within each objective to determine progress toward the individual objectives.
- Assess the collective progress of objectives to indicate progress toward overarching goals using the next statutorily required communications capabilities assessment in 2023.
- Compare results from the 2018 Nationwide Communications Baseline Assessment to the next assessment, measuring progress against key gaps identified in the NECP.
- Conduct a periodic collective assessment of the NECP goals and the 2023 Nationwide Communications Baseline Assessment to track progress toward the plan's overall implementation.

The NECP goals and objectives are designed to achieve the plan's vision—enabling the emergency response community to communicate and share information securely across communications technologies in real time, including all levels of government, jurisdictions, disciplines, organizations, and citizens impacted by any threats or hazards event. Progress toward achieving the NECP vision will be measured through the next Nationwide Communications Baseline Assessment. CISA conducts the assessment every 5 years to provide a national and statistically valid snapshot of public safety agencies' emergency communications capabilities and their current use, and to identify gaps that remain for interoperability to be achieved. The results of the assessment will gauge implementation of the NECP and will inform the development and update of the next iteration.

Reporting

In accordance with 6 U.S.C. § 1803, DHS is required to develop and submit the Biennial Progress Report on Emergency Communications to Congress. It is the official reporting mechanism that highlights the Department's specific accomplishments in carrying out its responsibilities under Title XVIII, as well as areas of progress, current gaps, and identified best practices for each element of the SAFECOM Interoperability Continuum and other critical areas identified by Congress. CISA will report progress on the NECP implementation through the Biennial Progress Report.

Conclusion

Since 2008, tremendous progress has been made to enhance emergency responder communications capabilities. However, the Nation must continue to build on previous successes and pursue opportunities for improvement. The NECP emphasizes the close collaboration of stakeholders to plan for and shape the future of emergency communications. The deployment of new technologies provides emergency responders access to high-speed and cutting-edge capabilities, while current emergency communications networks offer responders the security, reliability, and coverage they need to execute their mission in an all-hazards environment. Striking the right balance between addressing existing gaps and requirements while also integrating new technologies is a significant challenge facing public safety organizations across all levels of government.

The NECP sets forth six strategic goals to advance the capabilities needed for operational success in a dynamic and interconnected environment. The NECP establishes a series of targeted objectives that address each goal and collectively emphasize the maintenance and improvement of radio communications systems, integration of emerging IP-based technologies, and improved coordination among an expanding emergency response community. It also identifies success indicators as aspirations for stakeholders to achieve within their communities. For example, stakeholders will use the NECP to enhance and update the policies, governance structures, planning, and protocols that enable responders to communicate and share information under all circumstances. Ultimately, the intent of the NECP is to ensure the emergency response community drives toward a commonly defined end-state for communications.

Moving forward, emergency response agencies will be making critical decisions regarding resources, personnel, and equipment to address the evolving operating environment. The guidance provided in this plan will help to advance their efforts. However, success of the NECP will require the support and dedication of the entire emergency communications community, including government agencies, nongovernmental organizations, and citizens. In order to realize the NECP's vision, DHS will work diligently so the Nation's emergency responders and supporting entities can fulfill their mission as the Emergency Communications Ecosystem continues to evolve.

This page intentionally left blank.

Annex: Success Indicator Descriptions

This Annex expands upon the descriptions of the success indicators for the National Emergency Communications Plan (NECP) goals and objectives. The plan provides stakeholders with objectives to attain the NECP goals, as well as defines success indicators that result from achieving the objectives. These success indicators describe the desired future state of communications. Public safety organizations and partners should incorporate NECP goals and objectives into their local, regional, and state-level plans; identify appropriate actions to meet their unique needs and missions; and measure progress until success indicators are a reality. The Cybersecurity and Infrastructure Security Agency (CISA) will oversee NECP implementation in partnership with stakeholders from the public safety community.

Goal 1: Governance and Leadership. Develop and maintain effective emergency communications governance and leadership across the Emergency Communications Ecosystem

Objective 1.1: Formalize governance through policy, documentation, and adequate funding

Success Indicators

States and territories create or revise policy and plans to formalize and fund emergency communications governance bodies, such as Statewide Interoperability Governing Bodies

Formal governance structures (e.g., Statewide Interoperability Governing Bodies, State Interoperability Executive Committees, and Statewide 911 Boards) provide a foundation for public safety entities to collaborate, plan, and make decisions on strategies and operations that mutually support the investment, sustainment, and advancement of communications-related initiatives. Establishing statewide governance or revising the functions of existing bodies through statutes or Executive Orders formalizes the group's authority to make funding recommendations supported through the state's general funds or federal grant allocations. Without formal authority, ad hoc governance structures are vulnerable to disruption and loss of institutional knowledge as participation relies on volunteered time.

Governance bodies develop and implement governing documents, such as charters or bylaws, to clarify roles, purpose, authority, and methods for adapting to change

A charter or set of bylaws formally authorizes the existence of the governing body and provides a reference source for the future. Charters clarify governance operations, providing details on how to align the group's vision to a long-term strategy and their responsibilities for making decisions and implementing change. Additionally, effective charters clarify each participating organization's role, define administrative duties, and outline the organizational structure and voting processes for decision making in the group. The charter's value increases when members of the governance body seek buy-in on the document, encouraging commitment to the group's purpose and decision-making strategies. Additionally, charters with flexible language regarding adapting its membership, structures, and processes to the evolution of emergency communications tend to be the most valuable.

States and territories provide funding, authority, and governance to support a full-time Statewide Interoperability Coordinator in each state or territory, such as through the development of legislative language and mandates

The Statewide Interoperability Coordinator's primary function is to plan and implement the statewide interoperability program, guided by initiatives outlined in the NECP and the Statewide Communication Interoperability Plan. Statewide Interoperability Coordinators act as linchpins establishing and maintaining emergency communications governance and planning across each state or territory by bringing together stakeholders from a broad spectrum of public safety communications systems and services. As part of this effort, Statewide Interoperability Coordinators are responsible for the implementation of the Statewide Communication Interoperability Plan, which establishes a vision for interoperability across the state/territory. Statewide Interoperability Coordinators also execute the grant application process, coordinating decisions on communications investments funded through federal grants to ensure projects align with the Statewide Communication Interoperability Plans and are compatible with surrounding systems.

State and territory governance bodies prioritize communications needs and coordinate with the Statewide Interoperability Coordinator and other state-level planners on applications for federal financial assistance

In accordance with the SAFECOM Guidance on Emergency Communications Grants, states and territories are encouraged to coordinate with the Statewide Interoperability Coordinator and state-level planners (e.g., broadband and 911 planners, and utilities commissions), as well as the State Administrative Agency, to ensure projects and investments align with statewide plans and technical compliance requirements. The State Administrative Agency, or an equivalent role, is a principal figure for ensuring regional project plans are developed and implemented in coordination with contiguous jurisdictions; mutual aid partners; and other relevant partner organizations, jurisdictions, and sectors. The agency administers all homeland security and emergency communications grant funding for the state and, in coordination with the Statewide Interoperability Coordinator, is also a good resource for assisting with the Stakeholder Preparedness Review, regional and state strategic plans, and project alignment at the local level with the state's long-term vision for interoperability. For instance, the Statewide Interoperability Coordinator may escalate policy and grant recommendations to the State Administrative Agency for consideration by the Governor's Office.

Federal departments or agencies establish a federal interoperability office or designate a Federal Interoperability Coordinator

Emergency communications responsibilities at the federal level are often distributed across bureaus, components, offices, and programs. Few departments or agencies have governance mechanisms to implement interoperability policies, decisions, and processes. A designated emergency communications interoperability office, coordinator, or committee improves information sharing activities, better informs decision making, and provides a single point of coordination on interoperability issues for all partner agencies. This central authority leads initiatives across federal, state, local, tribal, and territorial partner agencies.

Objective 1.2: Structure more inclusive governance by expanding membership composition

Success Indicators

Governance bodies identify and include missing or underrepresented stakeholders (e.g., jurisdictions, tribes, sectors, and organizations) in formal governance structures, when developing strategic and operational plans and policies, and during training and exercises

Governance is only successful if those affected by emergency communications disruptions are directly involved in decision-making processes. However, governance in many areas still only involves traditional disciplines or sectors and excludes those responsible for secondary or tertiary systems or response functions. Non-traditional organizations responsible for public safety, emergency communications, or emergency services responding to area-specific hazards (e.g., forestry services in rural California, terrorism task forces in large urban centers) bring unique perspectives and challenges regarding interoperability. Increased collaboration with a wider variety of organizations results in reciprocal benefits, such as a larger inventory of available resources and knowledge between rural and urban communities. Successful coordination requires planning discussions across these entities through governance and the involvement of potentially under-represented organizations or sectors when developing strategic, operational, and contingency plans. For instance, public safety agencies from state/territorial, regional, and local governments and governance bodies benefit from strengthening relationships and establishing formal mechanisms for achieving interoperability with tribes. Such formal mechanisms could include establishing legislation for tribal representation on working groups and committees or memoranda of understanding or agreement to define how information, resources, and infrastructure may be shared. Involving tribal points of contact is necessary because tribes may also provide critical infrastructure support to surrounding jurisdictions or benefit directly from state/territorial, local, and regional infrastructure and emergency response capabilities.

Governance bodies include information management, network infrastructure, and cybersecurity representatives through membership or formalized coordination

Because of the increasing complexity of interconnected, Internet Protocol (IP)-based technologies and their integration into emergency communications systems, governance bodies and subgroups benefit from developing and implementing strategies, policies, and plans to assess, manage, and oversee the progression of risks and information management in the long term. Inviting information technology officers, such as the chief information officer, to participate in emergency communications governance bodies increases information technology services and public safety community end-user coordination. Additionally, establishing subcommittees related to new technologies, threats, and issues provides subject matter expertise when coordinating the integration and alignment of IP-based and advanced technologies.

Governance bodies coordinate with elected officials to champion public safety communications priorities and lifecycle planning among decision makers

Whether it be the elected official or a representative from his or her office, representation from these offices on formal public safety communications governance bodies allows those making fiscal and policy decisions to better understand priorities, take informed action, and advocate for resources. Formal collaboration gives elected officials and other decision makers greater access to and understanding of strategic plans and short- and long-term priorities, allowing them to contribute to the formation of solutions and necessary support for key priorities and challenges at state, local, tribal, and territorial levels. This approach emphasizes the need for direct discourse between public safety organizations and policymakers to determine a tangible path toward interoperability resilience.

Governance bodies coordinate and consult with tribal points of contact to develop cooperative strategies for achieving interoperability

Tribes continue to emphasize limitations to a "one size fits all" approach for partnering with their communities as tribe size, geographic location(s), experience, available resources, and challenges vary. Public safety agencies from state, territorial, regional, and local governments and governance bodies benefit from strengthening relationships and establishing formal mechanisms for achieving interoperability with tribes. Such formal mechanisms could include legislative establishment of tribal representation on working groups and committees and the establishment of memoranda of understanding or agreement to define how information, resources, and infrastructure may be shared. Involving tribal points of contact is necessary because tribes may also provide critical infrastructure support to surrounding jurisdictions or benefit directly from state, regional, and local infrastructure and emergency response capabilities.

Objective 1.3: Adopt adaptive governance strategies to address the rapid evolution of technologies, capabilities, and risks

Success Indicators

Governance bodies undertake technology integration and migration initiatives (e.g., broadband, 911, alerts and warnings, information management, network infrastructure, and cybersecurity) to guide implementation by public safety

As communications technologies converge, experts who oversee land mobile radio, broadband/long-term evolution, 911/Next Generation 911, alerts and warnings, information technology and security, social media, and other systems and services, work in tandem to strengthen emergency communications capabilities. Due to the overlapping nature of their positions, clarifying individual roles, as well as dependencies and collaborative functions, is key to avoiding duplication of efforts and ensuring consistent and coordinated deployment of technologies across existing systems. This approach ensures individual system plans (e.g., statewide 911 plans and cybersecurity strategies) align with the Statewide Communication Interoperability Plan and overall strategies for achieving interoperability.

Governance bodies identify and address legislative and regulatory issues associated with emerging technology

Implementation of new and emerging technologies require awareness and compliance with certain legislative and regulatory constraints surrounding public safety. For example, the First Responder Network Authority (FirstNet Authority) was required by statute to develop a national deployment plan for its Radio Access Network. However, it is important that governing bodies be aware of their own state's legislation that either limits or enables implementation of the network and its technology. Organizations should perform periodic reviews of federal, state, and local regulations affecting public safety and emergency communications technology in order to inform governing bodies and public safety organizations of funding opportunities, as well as any possible restrictions in securing emerging technology.

Organizations that support public safety communications formalize and regularly review cross-jurisdictional, multi-state, or multi-organizational agreements (e.g., memoranda of understanding, memoranda of agreement, and mutual aid agreements) to account for changes to resources, capabilities, and information- or technology-sharing needs

Memoranda of understandings, memoranda of agreement, or mutual aid agreements minimize risks for communities by supplementing informal relationships between agencies, which are often limited in scope and duration. However, few public safety organizations work with partner agencies to review and update emergency communications agreements on a regular basis. Written agreements, backed by formal governance, bring together multiple organizations and jurisdictions to establish common goals and objectives toward achieving operable and interoperable public safety communications. Agreements may also define party responsibilities for a shared system, provide its scope and authority, outline compliance issues, and even streamline processes for grant funding applications or awards. These agreements are most effective when reviewed regularly to account for changes to resources, capabilities, and information or technology sharing needs.

The Emergency Communications Preparedness Center serves as a decision-making body guiding lessons learned, best practices, and partnerships for federal organizations implementing new capabilities

Federal agencies with law enforcement and emergency response missions face ongoing challenges related to integrating new capabilities into their operations. The Emergency Communications Preparedness Center plays a valuable role assisting agencies to navigate challenges and realize opportunities associated with transitioning to new capabilities. Public safety organizations look to the Emergency Communications Preparedness Center to learn about how to more effectively share information on pilot programs and lessons learned, coordinate investments and acquisition strategies, and share systems, where possible.

Goal 2: Planning and Procedures. Develop and update comprehensive emergency communications plans and procedures that address the evolution of risks, capabilities, and technologies across the Emergency Communications Ecosystem

Objective 2.1: Develop and regularly update strategic plans to align with the NECP and address the integration of new emergency communications capabilities (e.g., voice, video, and data)

Success Indicators

Public safety organizations use strategic implementation plans (e.g., Statewide Communication Interoperability Plans, Regional Interoperability Communications Plans, Next Generation 911 Plans, and cybersecurity plans) to measure progress against NECP objectives and any additional state or territory objectives, and update plans annually

The Statewide Communication Interoperability Plan is the primary strategic implementation plan for each state and territory, defining critical emergency communications capabilities and needs. The Statewide Communication Interoperability Plan outlines the public safety community's recommendations on how to improve voice, video, and data communications across the state/territory through the development of vision and mission statements, milestones or activities to achieve specific goals, and a governance structure with specific roles and responsibilities assigned to those executing tasks in the plan. States and territories work with the Statewide Interoperability Coordinator to ensure investments support statewide plans and align with the NECP goals and objectives. Because many federal emergency communications grants require recipients to align their projects to the Statewide Communication Interoperability Plan and its Annual Snapshot, public safety agencies benefit by contributing to the development or revision of Statewide Communication Interoperability Plan content as it pertains to priorities across communities. An overarching statewide/territory-wide emergency communications plan helps states/territories align its stakeholders' efforts and focus resources toward activities and investments that will have the broadest and most profound impacts.

Federal departments or agencies develop emergency communications strategic plans in coordination with the Emergency Communications Preparedness Center

Given the rapidly evolving emergency communications and information technology environment, it is critical that federal departments and agencies plan for new investments, maintain and modernize legacy systems, and identify the personnel and training needs that are necessary to meet new challenges. Strategic plans and roadmaps enable an organization to document its vision for the benefit of staff and partner agencies, prioritize communications resources, strengthen governance structures, identify future communications investments, and resolve long-standing interoperability issues. While these plans often vary from agency to agency, the Emergency Communications Preparedness Center works with federal personnel to ensure they have the tools needed to develop, coordinate, and share strategic plans across the interagency community to identify opportunities for cooperation.

Objective 2.2: Align emergency communications funding and investments with strategic and lifecycle planning

Success Indicators

Federal funding authorities develop grant guidance for emergency communications governance and investments consistent with guidelines provided by SAFECOM and the NECP

Emergency communications guidelines such as the NECP and SAFECOM Guidance on Emergency Communications Grants are regularly updated to align with the newest emergency technologies and capabilities. In response, federal grant-making agencies (i.e., supporting emergency communications activities as an allowable cost) are encouraged to consistently update their federal grant guidance to accommodate these changes. Communicating and allowing grant applicants and recipients to fund the latest advancements in emergency communications technologies provide entities with the most up-to-date information to make sound, sustainable, and long-term investments in interoperability.

Public safety organizations develop and use lifecycle plans to inform agency funding decisions and implement new technologies while maintaining necessary legacy and backup systems

Successful lifecycle plans take each phase of SAFECOM and the National Council of Statewide Interoperability Coordinators' lifecycle planning model into account and include input from project planners, decision makers, and other stakeholders as necessary. Lifecycle plans also consolidate assessments performed to determine need for equipment or system sustainment and upgrade, dividing a large communications initiative into smaller projects for funding and implementation in phases over time. Due to the potential longevity of these plans, content should be reviewed and updated regularly to reflect changes in project status for planning purposes. Project planners developing implementation portions of the lifecycle plan, including dates, milestones, and roles and responsibilities, should refine content before and after the request for proposals process to ensure they are accurate and achievable. The DHS Lifecycle Planning Tool is available to help organizations plan accordingly.

Public safety organizations and governing bodies identify sustainable funding mechanisms to support the lifecycle planning model

Public safety organizations use a variety of funding mechanisms and resources in their efforts to prioritize system sustainment and upgrade. Detailed in the SAFECOM and the National Council of Statewide Interoperability Coordinators Funding Mechanisms for Public Safety Communications Systems are examples of alternatives to grant funds which include bonds, public-private partnerships, user fees, 911 surcharges, traffic ticket and vehicle surcharges, leasing equipment and infrastructure from public and private entities, and other unique streams. The Emergency Communications System Lifecycle Planning Guide also describes the lifecycle planning model and provides strategies for funding purchases, maintenance, and upgrades of systems.

Objective 2.3: Incorporate risk management strategies to protect against and mitigate disruptions to mission-critical communications

Success Indicators

Local public safety organizations work with state agencies to evaluate emergency communications threats, hazards, and needs in formal capability reporting mechanisms (e.g., Threat and Hazard Identification and Risk Assessment and Stakeholder Preparedness Review)

The DHS Threat and Hazard Identification and Risk Assessment and Stakeholder Preparedness Review are helpful when conducting state-level, emergency communications capability evaluations.

All types of communities participate in these interconnected processes to evaluate community preparedness. State and local decision makers and Statewide Interoperability Coordinators should apply information within these assessments to direct funding and sustainment resources to new and legacy emergency communications systems.

Public safety organizations incorporate risk management strategies into plans for continuity and recovery of critical communications

Determining and testing strategies to increase the resiliency of public safety networks and the knowledge of personnel who administer them, help to prevent catastrophic loss of critical communications to end-users during emergencies or disasters. Despite its importance, less than half of public safety organizations build processes into their plans to ensure continuity during out-of-the-ordinary emergencies or disasters. Continuity portions of plans identify the minimum communications requirements needed to perform essential functions, the availability of alternate equipment and systems, the designated staff and their responsibilities, and the location of facilities or bases. From a purely network-resiliency perspective, three key elements to consider when planning include: (1) route diversity, or routing between two points over one geographic or physical path with no common points; (2) redundancy, when additional or duplicate communications assets share the load or provide back-up to the primary asset; and (3) protective and restorative measures to decrease the likelihood a threat will affect a network (i.e., methods to enable rapid reestablishment of services if disabled or destroyed, such as DHS's Telecommunications Service Priority). Additionally, continuity of operations plans may provide details on pre-operational and operational procedures to protect assets, secure information and backup systems; recovery procedures, including identification of alternative communications systems available but not used during day-to-day operations (e.g., satellite); details on communications response and recovery teams; cross-training opportunities to address potential personnel shortages; Communications Unit leader training; emergency and service provider contact lists; and procedures for accessing priority services programs (e.g., Telecommunications Service Priority, Government Emergency Telecommunications Service, and Wireless Priority Service). When developing continuity of operations plans, public safety organizations should also consider communications operability, interoperability, resilience and security with respect to third-party service-level agreements and interconnection providers. In this new era of critical interconnection, public safety organizations must understand the providers' resiliency.

Public safety organizations that use information technology have a cybersecurity incident response plan in place

Incident Response Teams, incident response plans, recovery or resiliency plans, and continuity of operations plans are useful in cybersecurity incident responses. Information technology administrators may consider establishing a Computer Security Incident Response Team or reach an agreement with CISA's Incident Response Team to assist in cybersecurity planning. A Computer Security Incident Response Team serves as a central authority to report and analyze security issues within an organization. A team may also recommend potential solutions to the threats and publicize known threats, vulnerabilities, and solutions generally or to a specific information sharing community. The Computer Security Incident Response Team works with hardware and software vendors to obtain information about vulnerabilities and potential solutions. Additionally, coordinating response and recovery efforts with the Statewide Interoperability Coordinator and other information technology administrators can increase cybersecurity posture.

Public safety organizations perform resiliency assessments and mitigate vulnerabilities

According to the 2018 Nationwide Communications Baseline Assessment, poor coverage and system/equipment failure were some of the most common technical factors impacting public safety's ability to communicate. Communications continuity is a network's ability to withstand physical and cyber damage, thereby minimizing the likelihood of a service outage. Three key elements increase availability: (1) route diversity, (2) redundancy, and (3) protective/restorative measures. Performing physical and cyber resiliency assessments can help an organization ensure continuity of service in the event of an emergency, justify network operations and improvement funding requests, increase organizational control, and prioritize areas for network improvement. More information can be found in the Public Safety Network Communications Resiliency Self-Assessment Guidebook and Public Safety Communications Resiliency: Resiliency Ten Keys to Obtaining a Resilient Local Access Network.

In addition, radio frequency best practice implementation plays a critical role throughout the system lifecycle. Radio frequency coverage testing and analysis should be used to define and refine system coverage requirements, supplement baseline coverage studies (e.g., Coverage Acceptance Testing), provide in-building coverage measurement including assistance in locating interfering signals, and assist with system optimization, as well as ongoing maintenance. Resiliency assessments should account for the entire system lifecycle, including regular testing and maintenance. Encouraging accurate wireless coverage reporting, use of roaming agreements, and innovation and investment to enhance wireless network coverage for all users improves public safety.

Goal 3: Training, Exercises, and Evaluation. Develop and deliver training, exercise, and evaluation programs that enhance knowledge and target gaps in all available emergency communications technologies

Objective 3.1: Update and ensure the availability of training and exercise programs to address gaps in emergency communications

Success Indicators

Public safety organizations develop or update training and exercise programs to address new technologies, data interoperability, cybersecurity, use of federal and national interoperability channels, personally identifiable information, and continuity of communications

Standardized communications-focused objectives and evaluation criteria for training and exercise programs development requires a thorough understanding of existing gaps across all levels of government. The 2018 Nationwide Communications Baseline Assessment identified several issues that should be included in training and exercise programs, such as integrating existing systems with IP-based technologies and services, establishing processes for data management and exchange, addressing cybersecurity and other risks, increasing proficiency in end-users ability to program and use federal and national interoperability channels, and maintaining mission-critical communications during disruptions in operations. Updated training and exercise programs addressing these topics improve the public safety community's ability to increase capacity and build on existing capabilities.

Public safety personnel across multiple agencies and jurisdictions are registered for communications training classes and exercises whenever possible

Training and exercise programs help identify and mitigate communications challenges, but only if these programs tackle interoperability across the Ecosystem. Comprehensive programs address technology, process, and human factors related to interoperability; this applies not only to an agency's or entity's systems but also to those of partners, with a focus on where those systems intersect. Identified capability gaps and interoperability challenges can be incorporated into objectives, injects, and scenarios. Where possible, partners from across the whole community should be invited to attend as participants, staff, or observers. Serving as evaluation staff is a good way for partners to enhance one another's programs. The reliability of evaluations increases when third-parties observe, document, and report on outcomes. In return, evaluators are introduced to new processes, technologies, and best practices that they can take back to their home jurisdiction.

Public safety organizations coordinate training and technical assistance across levels of government (as applicable) to ensure current and consistent information

The CISA Regional Coordination and Technical Assistance Programs work with the public safety community to ensure training and technical assistance remain viable and current. Statewide Interoperability Coordinators have an understanding of training and technical assistance requirements within states and territories, and also help local, tribal, and individual organizations to identify and participate in training and technical assistance opportunities. Where training requirements cannot be fulfilled with in-state resources, Statewide Interoperability Coordinators coordinate and identify training resources with the state training authority (e.g., State Training Officer). Participation in regional and nationwide public safety groups and associations allows emergency communicators to ensure their organizations have current information regarding trainings and technical assistance offerings.

Public safety organizations include injects in exercises to test communications systems and personnel (including emerging technology and system failure) and utilize third-party evaluators with communications expertise

The public safety community reported the need for third-party or peer evaluators during exercises. Self-evaluations may be influenced by bias resulting in non-credible or false performance data. Given the proper tools (e.g., quality exercise evaluation guides) facilitators can accurately observe, appraise, and document the performance of tasks and activities that compose a capability. At the same time, independent third-party evaluators, with no connection to the players or their agencies, offer an additional level of objective evaluation. Partnering agencies that support each other with trainers, exercise controllers, and evaluators, benefit from these cross-agency interactions, which leads to improved trainings, exercises, and capabilities on all sides. Written agreements as to which party assumes costs related to these shared resources are beneficial to support continued use of third-party evaluators, controllers, and trainers.

Public safety organizations integrate private sector, nongovernmental organizations, and public sector communications stakeholders into training and exercises

Training with organizations from a broader range of disciplines and levels of government enhances interoperability, and by extension, preparation for events that involve numerous agencies. As reported in the 2018 National Communications Baseline Assessment, only 7 percent of public safety organizations report training with nongovernmental organizations and private-sector entities. In contrast, 23 percent report not training with any other types of organizations, with the remainder of organizations falling somewhere in between these extremes.

Nongovernmental organizations and private sector entities operate critical infrastructure that provides or supports emergency communications including operations centers, towers, generators, repeaters, and vehicles. Many nongovernmental organizations and private sector entities also maintain communications capabilities for day-to-day safety and security operations, as well as responses to out-of-the-ordinary events. In some cases, nongovernmental organizations (e.g., the American Red Cross) engage in day-to-day incident response that necessitates employing emergency communications technologies. Similarly, other supporting entities such as health and transportation agencies, routinely use voice and data capabilities to dispatch and communicate with personnel in the field. These entities may need to interoperate with public safety organizations during out-of-the-ordinary events to coordinate the deployment of resources and ensure their safety. Effective coordination among public safety organizations, nongovernmental organizations, private sector, and supporting entities require resource-sharing agreements and benefit from participation in joint training, exercises, and planned events, such as parades and communications rallies.

The Emergency Communications Preparedness Center analyzes gaps and identifies opportunities for federal interagency training and exercise programs

Due to the Federal Government's involvement in large-scale emergency preparedness and response, federal agencies manage, offer, and participate in an array of training and exercise programs aimed at improving the operability, interoperability, continuity, and security of communications capabilities. The Emergency Communications Preparedness Center is well positioned to analyze mutual capability gaps, develop common objectives, identify opportunities for joint trainings and exercises, and centrally track interagency progress.

Objective 3.2: Incorporate human factors in training and exercises to address the demands that voice, video, and data information place on personnel

Success Indicators

Public safety organizations implementing mobile data applications utilize training and tools to ensure that responders effectively use and are not overloaded by available information

New technologies being integrated into public safety communications are changing the nature of the jobs performed both in the field and at facilities such as public safety answering points and emergency operations centers. Information flow, volume, and sources of data are evolving; therefore, training programs need to address the use of new technologies and the impact of change on responders and their work. For example, video messaging changes the interaction of a public safety telecommunicator with a caller from a voice interaction to a face-to-face interaction. Physical reactions of the public safety telecommunicator such as facial expressions are no longer hidden from the distressed caller, necessitating a new set of skills and coping mechanisms for the public safety telecommunicator. In the field, new technologies such as body-worn cameras also require additional training for responders. Administratively, the changes that come with new technologies may require trainings for new approaches to screening and interviewing job applicants and during performance reviews. To ensure effective use of all available technologies when a responder is under the most stress, progressive training and exercise programs can be designed to build from previous lessons, adding new objectives along the way. Progressive training and exercises not only build upon each other, they also increase repetition of use to develop muscle memory, leading to the likelihood of available technologies being used appropriately and effectively during all events and incidents.

Public safety organizations implement tools and trainings to address emerging technology impacts

New technologies bring responders who are not on-scene closer to the impacts of a threat or hazard through photos, videos, and live streaming as events unfold. Public safety agencies will benefit from incorporating modules demonstrating techniques to combat compassion fatigue or vicarious trauma into trainings and building opportunities to practice those methods into exercises. Trainings and tools to develop emotional intelligence and peer support mechanisms can be added to programs. In many cases, introduction to these concepts can be delivered through internet-based learning applications that apply distance-learning techniques and can be viewed at the convenience of the responder. Effective tools and trainings address these mental health issues before exposure and following traumatic events.

Objective 3.3: Ensure training addresses information sharing (e.g., voice, video, and data) for multi-agency responses

Success Indicators

States, territories, and tribal nations implement programs (based on best practices) to oversee the qualification, training, certification, recognition, activation, and currency of communications-support personnel

A designated point of authority to oversee the qualification, training, certification, recognition, activation, and currency of Emergency Support Function #2 and Communications Unit personnel greatly improves the awareness, use, and tracking of trained personnel for response operations. Managing the tracking aspects of qualification, training, certification, recognition, and activation of communications support personnel is frequently overlooked. When training programs lack a proper tracking system for ensuring compliance of personnel, it creates confusion about overall readiness status (i.e., which personnel are active and ready for deployment).

States, territories, and tribal nations develop and support instructor cadres to expand training for communications-support personnel

Emergency Support Function #2 and communications support personnel are typically required during emergencies and planned events. To meet demand, organizations need to provide adequate training to new personnel and enable existing personnel to renew their qualifications, certifications, and credentialing. Increased support for communications instructor cadres will ensure communications-support programs have a sufficient number of accredited personnel at all times.

SAFECOM and the National Council of Statewide Interoperability Coordinators develop training curriculums for additional positions within the Information Technology Service Unit

After-action reports regularly document communications and information management challenges. Additionally, providing data connectivity at most incidents is common place; however, there is no specific person or place within the Incident Command System responsible for providing such personnel or resources. To simultaneously establish positive radio communications and network connectivity to manage the demand for digital information in multiple forms, new job positions and requisite curriculums are needed to support communications during all-hazards planned events and unplanned incidents.

Goal 4: Communications Coordination. Improve effective coordination of available operable and interoperable public safety communications capabilities for incidents and planned events

Objective 4.1: Confirm the implementation of the National Incident Management System

Success Indicators

Public safety organizations possess primary, secondary, and backup communications capabilities aligned with National Incident Management System Incident Command System and share appropriate forms (e.g., Incident Command System 205) illustrating the status of an agency's capabilities

As public safety organizations maintain, implement, upgrade, or replace existing communications capabilities, those capabilities should reflect an alignment with National Incident Management System Incident Command System doctrine to ensure available fielded capabilities are sufficient to support primary, secondary, and backup communications services required by planned events and incident responses.

As the scope of a reported incident becomes known, the communications capabilities required to coordinate the incident activities must be scaled appropriately to meet the on-scene communications needs while preserving enough capability and capacity for normal operations within the incident jurisdiction. Public safety organizations and discipline-specific communications requirements based upon the initial report of the incident type may alter established pre-plans and the normally or commonly used communications pathways. The evolving nature of a no-notice incident or damage to primary, secondary, or backup communications capabilities may alter the predetermined use of specific capabilities at an incident scene. As the initial units arrive, communications play a pivotal role in confirming and determining the type of incident, its scope, and the requirements for additional public safety resources. Depending upon initial observations and determinations, coupled with additional incoming information to the emergency communications center/public safety answering point, various communications resources may be pressed into service to support an evolving incident. Depending upon the incident size, scope, location, and evolution progress, the Incident Commander or Incident Management Team should remain well-informed about the status of all available operable and interoperable communications capabilities; information may be obtained through sharing appropriate Incident Command System form(s).

Public safety organizations assess and improve the timeliness of notification, activation, and response of communications systems providers to support the Incident Commander and Incident Management Team requirements at incidents and planned events

Anecdotal trends indicate public safety organizations are committing more resources during initial responses to reported critical incidents based upon better information-gathering from various reporting sources. These heightened responses require more and better pre-planning with competent and experienced Incident Commander/Incident Management Team personnel supported by communications systems providers and augmented by coordinated, robust, flexible, and resilient voice and data communications capabilities to effectively address incidents and planned events of all types and sizes.

Public safety organizations and Incident Commander/Incident Management Team personnel must be aware and comfortable with the amount of time it will take to acquire the important support of communications systems providers. Equally important, the criteria for event planning is evolving to ensure that public safety organizations effectively plan for contingencies where a planned event evolves into a critical incident.

As the complexity of communications systems increase due to the unrelenting pace of technological advances, it is important for public safety organizations to improve the inclusiveness of their communications systems providers to offer necessary technical assistance and advice to improve coordination and planning for planned events and incident response activities. Regardless of whether public safety organizations' communications systems providers are internal, external, or both, the expertise, knowledge, information, and access to additional communications resources can be the difference between a successful or failed incident response.

Objective 4.2: Enhance coordination and effective usage of public safety communications resources at all levels of government

Success Indicators

Public safety organizations maintain and readily share comprehensive information about features, functionality, and capabilities of operable and interoperable communication resources

The ability for public safety organizations at all levels of government and in every discipline to effectively communicate is crucial when delivering critical, lifesaving services. To coordinate various communications tools, knowing the availability and current state of all operable and interoperable assets is critical. At a minimum, all public safety organizations need to share current communications systems information with contiguous public safety agencies as well as other organizations who may provide or receive automatic aid or mutual aid, share infrastructure or resources, or participate in planned events. This sharing of active, available features, functionality, and capabilities of current communications resources can expedite communications coordination for both incidents and planned events.

Public safety organizations use up-to-date defined practices, procedures, pre-plans, specific venue/location response plans, incident type response plans, standard operating procedures, tactical response directives, and/or Tactical Interoperability Communications Plans that identify primary, secondary, and backup communications assets (e.g., networks, devices, and applications) for effective communications coordination and information sharing during planned events and incidents

Public safety organizations of various disciplines use a variety of practices, defined plans, and procedures to delineate voice and data communications capabilities available for incident and event communications coordination. These practices, plans, procedures, and the accuracy and completeness of the information therein can vary widely depending upon the involved agencies' size, location, sophistication, and established cooperation with other contiguous or non-contiguous agencies. As the scope of an evolving incident increases or a planned event requires communications assets and personnel from greater distances, Incident Commanders and communications providers must continually assess the best communications capabilities to incorporate in the incident management plan(s) or planned event criteria. These assessments can be essential in completing necessary Incident Command System forms that effectively communicate the categories, types and availability of primary, secondary, and backup communication capabilities available.

Public safety organizations periodically evaluate, engage, and incorporate commercial and non-traditional communications partners (e.g., auxiliary communications, volunteers, and utilities) in incidents and planned events

To enhance communications coordination, public safety organizations should evaluate existing communications policies, plans, agreements, and current systems and capabilities usage to determine appropriate inclusion of commercial and non-traditional communications partners and providers. Through this assessment, public safety organizations determine opportunities for improvements to communications coordination available through these entities. Moreover, these commercial and non-traditional partners and providers should be included in event and incident planning functions so that their resources are readily engaged when needed.

The state-level alerting authority and relevant lower-level alerting authorities ensure the highest state of readiness of existing capabilities for resilient and interoperable alerts, warnings, messaging and notifications using current local, county, state, and federal systems, and, when applicable, the Integrated Public Alert and Warning System (IPAWS)

It is important for all alerting authorities to issue timely critical public alerts, warnings, messaging, and notifications. Alerting authorities should establish and execute repetitive periodic testing procedures for alert, warning, notification, and messaging systems to ensure proper performance and highest systems readiness. Such testing should also include specific opportunities to periodically observe and record the proficiency of systems users that are generating and distributing alerting information.

The Federal Emergency Management Agency's IPAWS is an internet-based capability that federal, state, local, tribal, and territorial authorities can use to enhance existing capabilities to issue critical public alerts and warnings. It does not replace existing alerting, warning, messaging, and notification methods; instead, it complements existing systems and may provide new capabilities.

Objective 4.3: Develop or update operational protocols and procedures to support interoperability across new technologies

Success Indicators

Public safety organizations develop and regularly update National Incident Management System-aligned standard operating procedures to facilitate the integration, deployment, and use of communications assets

As noted in the 2018 Nationwide Communications Baseline Assessment findings, few agencies have developed interoperability policies for emerging communications technologies—only 20 percent of standard operating procedures cover Next Generation 911; 18 percent cover broadband; 18 percent cover priority services; and 16 percent cover cybersecurity. Clear and effective standard operating procedures enable personnel from across the Ecosystem to successfully coordinate for planned events and unplanned incidents. Additionally, standard operating procedures with mission- or capability-specific roles require coordination across agencies to standardize procedures in the event of an incident requiring cross-jurisdictional response.

The National Incident Management System includes communications tactical requirements and resources in the incident action plan. Incident Command System Form 205 serves as the tool to ensure incident responders have the necessary resources, including equipment, frequencies, and other assets that may be in short supply during a large-scale event. While completing Incident Command System Form 205 is important, sharing the Incident Action Plan, which includes Form 205, is imperative to ensure communications are interoperable and resources align to objectives. When an event is planned or slow-forming, agencies share Incident Action Plans in advance so that adjustments can be made in a timely manner. Even when operational periods are short and Incident Action Plans are produced quickly, planning personnel must work with Communications Unit personnel to ensure resources are distributed appropriately and all section chiefs ensure the Incident Action Plan is shared with incident responders. Incident Commanders and section chiefs promote the need for communications planning at the tactical level.

Public safety organizations have recommended guidelines regarding the use of personal devices (e.g., bring your own device) based on applicable laws and regulations

The proliferation of personal mobile devices and implementation of network policies, such as bring your own device, require strong authentication, data encryption, and consistent policies and configuration guidance in order for organizations to remain secure and interoperable. Public safety organizations should create and enforce mobile device policies regarding accreditation, acquisition, provisioning, configuration, use of encryption, monitoring, control, service management, security management, expense management, customer care, retirement, and reuse of mobile devices. In addition, public safety organizations should consider the use of mobile device management solutions that address configuration management, software patches, audio/video permissions, device-level intrusion detection and prevention, and digital asset management systems (e.g., sandbox, virtual desktop). Working with vendors to develop mission-related use cases and requirements to inform comprehensive mobile device management solutions can also improve implementation of these solutions. DHS's Mobile Device Adoption Best Practices Guide provides introductory best practices for organizations considering mobile device use, though organizational-level guidance should be in compliance with applicable laws and regulations. In addition, bring-your-own devices should maintain capabilities that meet both operational needs and any necessary evidentiary standards.

Public safety organizations leverage training, exercises, and real-world events to test capabilities and update standard operating procedures

Real-world events, whether planned or unplanned, provide opportunities to translate standard operating procedures from policy to practice and test their aptitude for establishing and maintaining communications during an emergency or disaster event. For instance, multi-organizational communications planning bodies benefit from developing documentation prior to planned events to capture the operationalization of emergency communications systems. These efforts include clarifying roles, sharing applications, developing channel plans, collecting and processing historical information and institutional knowledge, and establishing coordination processes for interoperable talkgroups and sharing of assets. Technology advancements also require capabilities to be tested and standard operating procedures to be updated. For example, voice and data encryption usage is increasing throughout the public safety community. The decision to use encrypted interoperable communications must be made with the understanding that encryption can add a significant level of complexity and should be considered only when the operational requirements of the incident outweigh the additional complications.

In addition, managing the associated encryption keys across their lifecycle can result in additional vulnerabilities and could possibly make important data inaccessible to authorized users.[7] Guidance on encryption and key management is available to the community, such as the Best Practices for Public Safety Interoperable Communications.[8] Processes developed to test the use of existing or new technologies may be exercised during scenarios, leading to standard operating procedures resolution prior to real events. Agencies develop after-action reports following events to assist with defining gaps or missing information resolved through the development or revision of standard operating procedures.

Public safety organizations periodically review their use of Priority Telecommunications Services (e.g., Telecommunications Service Priority, Government Emergency Telecommunications Service, and Wireless Priority Service) and FirstNet, and ensure they have standard operating procedures governing the programs' use, execution, and testing

Government Emergency Telecommunications Service provides emergency access and priority processing on the local and long-distance portions of the Public Switched Telephone Network for National Security/Emergency Preparedness users. Wireless Priority Service provides National Security/Emergency Preparedness personnel priority access on wireless networks. The Telecommunications Service Priority Program, one of the Priority Telecommunications Services, gives National Security/Emergency Preparedness users priority treatment of their telecommunications service requests in the event of service disruption. Employing these services can improve continuity of communications.

Public safety organizations periodically assess the proficiency of personnel in using communications systems' features, functions, and capabilities

Public safety organizations should establish and maintain a repeatable process to periodically observe and record the proficiency of users of primary, secondary, and backup communications systems. This includes an end-user's ability to properly access, navigate, manipulate, and use available features, functions, and capabilities of their communications devices and equipment. Observations that illustrate a user's lack of proficiency in the use of communications capabilities should drive appropriate modifications and expansion of user instructional documentation, informal and formal trainings, drills, exercises, and standard operating procedures.

[7] The use of voice encryption on designated interoperability and mutual aid channels can create obstacles to interoperability and is highly discouraged. In the event encryption is deemed necessary due to unique operational needs, it must follow existing Federal Communications Commission regulations and comply with an approved regional communications plan.

[8] National Public Safety Telecommunications Council's Best Practices for Public Safety Interoperable Communications, Best Practice #11 Managing Encryption for Interoperability Resources: The use of voice encryption on designated interoperability and mutual aid channels can create obstacles to interoperability and is highly discouraged. In the event encryption is deemed necessary due to unique operational needs, it must follow existing Federal Communications Commission regulations and comply with an approved regional communications plan. National Public Safety Telecommunications Council Report: Best Practices for Public Safety Interoperable Communications, May 2018.

Objective 4.4: Strengthen resilience and continuity of communications throughout operations

Success Indicators

Public safety organizations establish sufficient testing and usage observations of all operable and interoperable primary, secondary, and backup communications systems

It is important for public safety organizations to establish a repetitive periodic testing procedure for all operable and interoperable communications resources (e.g., primary, secondary, and backup) to confirm highest availability and readiness of those resources. For primary systems, usage observations in lieu of testing are sufficient to ensure the highest degree of availability. Processes to ensure proper notification procedures need to be established to alert communications systems providers for timely repair responses and to inform end-users of any failures or unavailability of a communications feature, function, or capability.

Emergency communications centers/public safety answering points address systems and staffing to support communications continuity-of-operations planning

As part of continuity-of-operations planning, emergency communications centers/public safety answering points should address the staffing requirements and technical resources needed to support their ability to maintain communications and functions during incidents and planned events. This includes succession planning as well as backup procedures for major systems, such as computer-aided dispatch, radio, and power supply. In addition, emergency communications centers/public safety answering points continuity of operations planning should incorporate relevant capabilities and assets, such as the Telecommunicator Emergency Response Task Forces initiative. Telecommunicator Emergency Response Task Forces can help states/territories develop programs to train teams that can be quickly mobilized and deployed to assist communications centers in the aftermath of disasters. These efforts can strengthen centers' ability to maintain continuity as the public's main point of contact during crises, while also serving as key coordinators of emergency management activities by dispatching information to responders.

SAFECOM and the National Council of Statewide Interoperability Coordinators develop best practices to encourage active network sharing and regionalization of shared services

SAFECOM and the National Council of Statewide Interoperability Coordinators' Shared Communications Systems and Infrastructure approach focuses on creating the plans, processes, and structures to enhance communications operability, interoperability, security, and continuity throughout the Nation. There are several benefits of network sharing, including improved spectrum use, optimization of resources, positive environmental impacts, a decrease in duplicate investment, reduction of capital and operational expenditure, streamlined interagency operations, enhanced operational coordination, and economies of scale for subscriber units.

Goal 5: Technology and Infrastructure. Improve lifecycle management of the systems and equipment that enable emergency responders and public safety officials to share information efficiently and securely

Objective 5.1: Support public safety requirements that drive research, development, testing, and evaluation of emergency communications technology

Success Indicators

SAFECOM and the National Council of Statewide Interoperability Coordinators identify public safety technology and infrastructure capability gaps

Public safety communications benefit from a validated national perspective on capability gaps. SAFECOM and the National Council of Statewide Interoperability Coordinators identify capability gaps that impact the operability, interoperability, and security of public safety communications, then provide the capability gaps to the Emergency Communications Preparedness Center, which addresses how gaps can be resolved through existing technology, technological research and development, and marketplace innovation. Capability gaps are also addressed through public safety organizations' governance, standard operating procedures, training and exercise guidance, and usage/testing advancements. In addition, the Telecommunications Industry Association is convening an ongoing open process on software component transparency to provide better visibility into the software supply chain.[9] SAFECOM and the National Council of Statewide Interoperability Coordinators have the opportunity to facilitate public safety input and participation into the development of the stakeholder documents.

The Emergency Communications Preparedness Center coordinates federal research, development, testing, and evaluation priorities and processes

With organizations often facing common technology challenges, the Emergency Communications Preparedness Center can help coordinate these activities by maintaining a database of research and development projects on its Federal Emergency Communications Research and Development Portal. In addition, the Emergency Communications Preparedness Center can conduct joint initiatives and assessments, as well as drive multi-agency participation in testing programs. The Emergency Communications Preparedness Center provides a forum for member agencies to (1) coordinate efforts with research centers and laboratories that develop and test new communications technologies; (2) coordinate with organizations conducting research and development to address DHS Component requirements, including those that partner with other public safety organizations to extend this research to meet their needs; and (3) coordinate with programs that evaluate the reliability and effectiveness of commercially developed solutions for public safety use. A coordination point for research, development, testing, and evaluation efforts can prioritize activities that pose the greatest operational benefit to public safety, increase return on investment, and reduce time to market.

[9] Information on the Telecommunications Industry Association's activities can be found at https://www.tiaonline.org/.

The Emergency Communications Preparedness Center cultivates sustained engagement (e.g., cooperative agreements) between federal research, development, testing, and evaluation programs (e.g., DHS's Science and Technology Directorate and the National Institute of Standards and Technology's Public Safety Communications Research Division, and public safety organizations focused on resiliency, interoperability, and other challenges)

With limited resources, state, local, tribal, and territorial organizations are often limited in their ability to develop new technologies. Through laboratories and testing environments, the Federal Government plays a leading role in helping to research, develop, test, and evaluate communications technology for the entire public safety community. Engagement includes greater collaboration between the Emergency Communications Preparedness Center Working Groups and the SAFECOM Technology Policy Committee to ensure that federal programs are meeting and reflecting a broad cross-section of stakeholder concerns. The Emergency Communications Preparedness Center also encourages federal programs to regularly engage through conferences, summits, pilot projects, and cooperative agreements, such as those held by organizations like DHS's Science and Technology Directorate and the National Institute of Standards and Technology's Public Safety Communications Research Division. The Emergency Communications Preparedness Center has increased cross-collaboration with the Public Safety Communications Research Division on initiatives related to resiliency and capacity building to further identify critical communications technology gaps. Increased interaction with industry and stakeholders (e.g., communications and information technology sector-specific councils and information sharing and analysis centers, cross collaboration with SAFECOM) helps to identify key focus areas. Sustained engagement allows for strategic technology partnerships that meet public safety capability gaps for the whole community

The Emergency Communications Preparedness Center partners with the private sector to foster an open, innovative, and standards-based commercial marketplace for solutions development and ensures that public safety requirements are addressed in current and emerging standards

While direct federal investment in research and development is important to technology development, private industry plays a critical role by developing innovative systems, devices, and applications for the public safety market. Public safety organizations must have opportunities to ensure that the commercial public safety communications market is open, transparent, and informed on the priorities of public safety customers. Federal testing facilities can provide a controlled environment for industry engineers and public safety representatives to evaluate the performance of their solutions against public safety standards. Compliance certification programs can provide industry with an opportunity to demonstrate the compliance of new devices and applications with critical technology standards for public safety voice and data systems; they also provide public safety agencies with transparent documentation that standards are fully supported before they engage with vendors. Federal agencies can help coordinate industry engagement by funding pilot programs for new systems, devices, and applications that target the priorities of the public safety community and ensuring that the findings of those pilot programs are disseminated openly and transparently to public safety stakeholders. Priority Telecommunications Service and communications service providers can partner to ensure that priority service offerings keep pace with commercial deployment of IP networks, including 5G technologies. Public safety organizations can collaborate with industry and standards development organizations to ensure requirements are incorporated into emerging technology—greatly reducing future costs and re-engineering challenges. For example, the National Telecommunications and Information Administration is convening an ongoing open process on software component transparency to provide visibility into the software supply chain and has invited public safety organizations to participate in development.

Objective 5.2: Ensure communications and information sharing systems meet public safety's mission-critical needs

Success Indicators

SAFECOM and the National Council of Statewide Interoperability Coordinators communicate emerging technology impacts to public safety, such as those associated with identity management, multimedia, 5G, Internet of Things, social media, network virtualization, spectrum optimization, artificial intelligence, machine intelligence, geographic information systems, and positioning, navigation, and timing systems

The results of research and development, testing, evaluation, standards development, and early adoption of emerging technology must be communicated to the broader public safety community in plain language. SAFECOM and the National Council of Statewide Interoperability Coordinators best practices and educational guidance allow the community to harness emerging technology benefits, while also preempting or mitigating the risks associated with wide-scale deployment.

SAFECOM and the National Council of Statewide Interoperability Coordinators guide standards-based land mobile radio evolution

The Project 25 suite of standards for land mobile radio support interoperability and communications continuity for the public safety community. SAFECOM and the National Council of Statewide Interoperability Coordinators continue to support Project 25 standards development for interoperability; they encourage organizations that are purchasing Project 25 communications equipment to use the resources made available by the Project 25 Compliance Assessment Program. DHS, as the senior federal partner in the Project 25 standards development process and the chair of the Project 25 Steering Committee, continues to help drive interoperability testing, the addition of enhanced security features, and support for future communications capabilities such as Project 25 to long-term evolution interfaces.

Public safety organizations support the development and implementation of resiliency standards and guidelines to protect against events such as natural disasters, network and grid failures, terrorism, lightning, and electromagnetic pulse events

Government and public safety entities rely on voice and data communications networks to achieve their missions. Access to reliable communications services during times of emergency is critical to enable the public to request support and to allow response organizations to perform their functions. Natural disasters such as the 2017 Atlantic hurricane season, which resulted in a loss of more than 90 percent of the commercial, public safety, and governmental communications systems in Puerto Rico, and other events such as network and grid failures, terrorism, lightning, and electromagnetic pulse events affect public safety. The March 2019 Executive Order on Coordinating National Resilience to Electromagnetic Pulses underscores the importance of resilient infrastructure. Public safety-specific guidance, such as the Public Safety Network Communications Resiliency Self-Assessment Guidebook and Public Safety Communications Resiliency: Resiliency Ten Keys to Obtaining a Resilient Local Access Network, can help public safety organizations establish a process to assess threats and vulnerabilities to communications networks. Resiliency standards, such as American National Standard Institute candidate 2.106.1-201x Public Safety Grade Site Hardening Requirements, continue to evolve. Public safety organizations' engagement is critical in the development and implementation of resiliency standards and guidelines.

The FirstNet Authority innovates and integrates broadband technology into the Nation's public safety communications infrastructure

The FirstNet Authority is responsible for ensuring the successful deployment, operation, improvement, and financial sustainability of the nationwide broadband communications platform. The FirstNet Authority is also responsible for the advancement or enhancement of public safety communications through standards-based technology delivery, innovation, and participation in standards bodies related to emergency services and interoperability. To support this work, the FirstNet Authority engages with federal, state, tribal, and local public safety entities and works with national public safety associations that are members of the FirstNet Public Safety Advocacy Committee to understand their trends, drivers, and priorities. These public safety engagements allow the FirstNet Authority to remain current on user needs and to help public safety entities better understand how they can maximize the value they derive from FirstNet. FirstNet delivers specialized features to public safety such as priority access, preemption, end-to-end encryption, quality of service, more network capacity, and a resilient, hardened connection supported by dedicated infrastructure.

The National 911 Program coordinates, in collaboration with all levels of government, the optimization of 911 services, including the Nation's transition to Next Generation 911

The Department of Transportation National Highway Traffic Safety Administration's 911 Program Office plays an active role in coordinating and contributing to 911 policies, standards, and technology development through its work with public safety organizations across the country. The office coordinates with the Federal Communications Commission, which promotes public safety by encouraging and coordinating development of a nationwide, seamless communications system for emergency services, including making 911 the universal emergency number. It also provides strategic planning for collection and use of nationwide 911 data, offers guidance for interstate implementation of Next Generation 911, and administers the 911 Grant Program jointly with the National Telecommunications and Information Administration, a bureau of the Department of Commerce. The National 911 Program Office and SAFECOM and the National Council of Statewide Interoperability Coordinators have partnered on the promotion of consistent terminology and assessment of Next Generation 911 maturity, as well as guidance on Cyber Risks to Next Generation 911 Systems. The 911 Program Office also chairs the Next Generation 911 Working Group within the Emergency Communications Preparedness Center. This working group is currently working to complete a report that inventories federal emergency communications center/public safety answering point assets across the Nation.

Objective 5.3: Support data interoperability through the development of effective and sustainable information sharing and data exchange standards, policies, and procedures

Success Indicators

Public safety organizations employ standards-based information exchange models and data sharing solutions

To communicate seamlessly with the increasingly interconnected systems of the broader community, public safety organizations should use standards-based information exchange models, such as Organization for the Advancement of Structured Information Standards Emergency Data eXchange Language, National Information Exchange Model, Structured Threat Information eXpression/Trusted Automated eXchange of Indicator Information, and Global Reference Architecture.

Using these models can reduce the total cost of ownership of exchanging information among organizations, increase interoperability, improve grant-eligibility, and provide leverage community-wide for standards-compliant infrastructure. IPAWS has exemplified data interoperability through the development of effective and sustainable information sharing and data exchange standards, the Common Alerting Protocol standard. It is currently available in a network of 1,230 alert authorities nationwide, which continues to expand. Public safety organizations should also enable the interoperability of evolving technologies (e.g., FirstNet, Next Generation 911) by ensuring the bilateral transfer of data and information using evolving standardized interfaces.

Public safety organizations follow acquisition best practices, including consideration for standards-based infrastructure

Acquiring standards-based infrastructure in a multi-vendor environment supported by compliance testing minimizes the risk of operability and interoperability challenges. Standards-based infrastructure often supports a consistent set of security features, which can improve the security posture of the entire Ecosystem. After defining clear and concise requirements, public safety organizations use generic or non-proprietary language, as appropriate, to develop acquisition documents and consider the need for standards-based, interoperable, secure infrastructure during solution selection. Additional acquisition practices can be found in the 2018 Emergency Communications System Lifecycle Planning Guide.

SAFECOM and the National Council of Statewide Interoperability Coordinators publish best practices and updated guidance on standard operating procedures to help the public safety community overcome data storage, exchange, maintenance, and analysis challenges

The standards, policies, and procedures for data sharing range from informal verbal agreements to formal written documentation to standardized interfaces enabled by technology. The guidelines are developed by organizations at various levels of government and by dedicated organizations specially formed to improve data sharing capabilities. As reported in the 2018 Nationwide Communications Baseline Assessment, many local and tribal public safety organizations follow local-level guidance to develop their standard operating procedures. This indicates that most public safety organizations' emergency communications at the local-level are influenced by their own set of standards, policies, and procedures. To assist organizations nationwide, SAFECOM and the National Council of Statewide Interoperability Coordinators will develop best practices on data lifecycle management to improve data usage, interoperability, and security across the Ecosystem.

Goal 6: Cybersecurity. Strengthen the cybersecurity posture of the Emergency Communications Ecosystem

Objective 6.1: Develop and maintain cybersecurity risk management

Success Indicators

Public safety organizations, at a minimum, implement the National Institute of Standards and Technology Cybersecurity Framework

The National Institute of Standards and Technology Cybersecurity Framework is a flexible, risk-based approach to improving the security of critical infrastructure. Collaboratively developed between government and the private sector, the Framework is designed to complement an existing risk management process, or to develop a credible program if one does not exist. Public safety cyber risk programs should be coordinated with existing and future DHS Threat and Hazard Identification and Risk Assessment and Stakeholder Preparedness Review requirements. Ideally, organizations using the Framework and Threat and Hazard Identification and Risk Assessment/Stakeholder Preparedness Review will be able to measure and assign values to their risk, along with the cost and benefits of steps taken to reduce risk to acceptable levels. The better an organization can measure its risk, costs, and benefits of cybersecurity strategies and steps, the more rational, effective, and valuable its cybersecurity approach and investments.

Public safety organizations perform a Cyber Resilience Review

A Cyber Resilience Review is a no-cost, voluntary, non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices. The Review may be conducted as a self-assessment or as an on-site assessment facilitated by CISA cybersecurity professionals. The Review assesses enterprise programs and practices across a range of ten domains including risk management, incident management, service continuity, and others. The assessment is designed to measure existing organizational resilience as well as provide a gap analysis for improvement based on recognized best practices for federal, state, tribal, territorial, and local departments and agencies in the Emergency Services Sector using the National Institute of Standards and Technology Cybersecurity Framework.

Objective 6.2: Mitigate cybersecurity vulnerabilities

Success Indicators

SAFECOM and the National Council of Statewide Interoperability Coordinators share planning and mitigation guidance regarding known threats and vulnerabilities

In addition to promoting CISA's Incident Response Team and other Information Sharing Environment notifications of public safety-specific threats and vulnerabilities, SAFECOM and the National Council of Statewide Interoperability Coordinators guidance and participation in other stakeholder efforts educates the community on known threats and their mitigations. For example, botnets and automated, distributed attacks threaten the Nation's internet infrastructure and this directly affects the public safety community.

To address these threats, the Department of Commerce and DHS developed a roadmap that charts a path forward for coordination among government, civil society, technologists, academics, and industry sectors. SAFECOM and the National Council of Statewide Interoperability Coordinators can both ensure that public safety organizations are well-represented in the next iteration of the roadmap, while also conveying the protective actions that result from the work items produced from the road map efforts. Depending on the threat, SAFECOM and the National Council of Statewide Interoperability Coordinators guidance could also encourage risk mitigation through the implementation of current network management techniques, such as virtual private networks, access control systems, firewalls, segmentation, or continuous monitoring systems, to decrease public safety network vulnerability and identify areas for necessary research and development.

SAFECOM and the National Council of Statewide Interoperability Coordinators encourage cybersecurity for Next Generation 911

Next Generation 911 networks introduce new vectors for attack that can disrupt or disable operations. As such, SAFECOM and the National Council of Statewide Interoperability Coordinators produced community guidance on how to mitigate Cyber Risks to Next Generation 911 Systems. In addition, the Federal Communications Commission's Task Force on Optimal Public Safety Answering Points Architecture recommended the implementation of Emergency Communications Cybersecurity Centers.[10,11] Emergency Communications Cybersecurity Centers detect, analyze, and respond to cybersecurity incidents using a combination of technology solutions, security analysts, and a strong set of processes to serve any emergency communication services that would benefit from using centralized, core cybersecurity services. The Emergency Communications Cybersecurity Center cybersecurity layer for the Next Generation 911 architecture will play a vital part in the operation and maintenance of Next Generation 911. SAFECOM and the National Council of Statewide Interoperability Coordinators' expertise is vital to refining fundamental attributes of Emergency Communications Cybersecurity Centers, including governance, funding, usage, operating procedures, technical capabilities, technical architecture, and interconnection requirements. The Emergency Communications Cybersecurity Center layer must provide defined value for public safety answering points—compelling benefits to help them address cybersecurity and, potentially, the Big Data issues associated with acceptance of data-based communications, such as texts, photos, and videos.

Public safety organizations leverage ongoing efforts by the National Institute of Standards and Technology and standards development organizations to identify and mitigate equipment and protocol vulnerabilities that impact the public safety mission

One of the most important aspects of cybersecurity for the evolving emergency communications environment is the review of the equipment, standardized protocols, and proprietary mechanisms connecting devices to and through the internet. Not only will protocols and mechanisms need to be secure, but device manufacturers and system administrators will need to understand the importance of cybersecurity in an interconnected network environment, even when it impacts the simplicity and efficiency of their products.

[10] Federal Communications Commission Task Force on Optimal Public Safety Answering Point Architecture, Adopted Final Report. 29 Jan 2016, https://transition.fcc.gov/pshs/911/TFOPA/TFOPA_FINALReport_012916.pdf
[11] Federal Communications Commission Task Force on Optimal Public Safety Answering Point Architecture Emergency Communications Center, Optimal Cybersecurity Approach for Public Safety Answering Points, 2 December 2016, https://transition.fcc.gov/pshs/911/TFOPA/TFOPA_WG1_Supplemental_Report-120216.pdf

Evaluations may include supply and repair chain risk management, as well as deployment, operations, and maintenance guidance. Public safety organizations should leverage the continuous work performed by National Institute of Standards and Technology and standards development organizations, such as 3rd Generation Partnership Project, International Telecommunication Union – Telecommunications, and Alliance for Telecommunications Industry Solutions, to review protocol vulnerabilities.

Objective 6.3: Determine public safety-specific, standards-based cyber hygiene minimums and fund ongoing risk mitigation

Success Indicators

The National Institute of Standards and Technology's Public Safety Communications Research Division establishes recommended public safety-specific, standards-based cyber hygiene minimums for public safety

Cybersecurity is not a static process to be completed once, but a continual process of enhancing defense. Some organizations will have less capacity than others to apply for and manage grants, and therefore, public safety should leverage ongoing National Institute of Standards and Technology work to plan for setting, testing, and maintaining cyber minimum standards to assist cybersecurity-eligible grant programs in distributing necessary funding to public safety. According to the 2018 Nationwide Communications Baseline Assessment results, 37 percent of respondents indicated that cybersecurity incidents have had an impact on the ability of their emergency response providers and government officials to communicate over the past five years. Yet, almost half of respondents had not instituted cybersecurity best practices, such as risk assessments, continuous monitoring, and identity management. In fact, only one in five respondents indicated having cybersecurity incident response plans, policies, and capabilities.

SAFECOM updates the Interoperability Continuum to account for cybersecurity

To promote the importance of cybersecurity to operability and interoperability, cybersecurity should be included as a critical success element or within the lanes of the SAFECOM Interoperability Continuum. The Continuum helps emergency response organizations and policymakers plan and implement interoperability solutions for data and voice communications.

SAFECOM and the National Council of Statewide Interoperability Coordinators consolidate and publish information on cybersecurity services and grant programs, such as those detailed in the DHS Cybersecurity Services Catalog and the Homeland Security Grant Program

As detailed in the DHS Cybersecurity Services Catalog for State Local Tribal and Territorial, the Federal Government offers voluntary, non-binding, and no-cost cybersecurity services to state, local, tribal and territorial governments. In addition, public safety organizations may leverage Homeland Security Grant Program State Homeland Security Program and/or Urban Area Security Initiative grants for their cybersecurity risk management. The 911 Grant Program might also provide funds for cybersecurity solutions as part of broader operation of Next Generation 911 systems.

CISA studies the cost of cyber incidents in support of cybersecurity risk management

In the 2018 National Association of State Chief Information Officers study, state chief information officers identified reduction of risk to their state as the top criteria by which their success should be measured. Instead, the top criteria by which chief information officers reported that their success was actually measured was delivering cost reductions to their state. The National Association of State Chief Information Officers found that given the continued fiscal pressures on the states, this emphasis is not surprising. The ability to measure and reduce risk as cost-effectively and efficiently as possible is likely to remain an important requirement for the foreseeable future. CISA's Office of the Chief Economist is conducting a multi-sector analysis to understand the financial impacts of cyber incidents to inform cyber risk management and cybersecurity investment decisions. By reviewing historical data of the costs associated with cyber incidents, the Office of the Chief Economist is developing a defensible basis for evaluating loss avoidance. This information will be used to inform the forward-looking analysis of the benefits of cybersecurity investment.

The National Institute of Standards and Technology's Public Safety Communications Research Division provides incentives for public safety-specific, cybersecurity-specific research and development activities based on known threats

Government and academic research facilities identify and develop new technologies that address public safety mission-critical cybersecurity requirements that are not currently offered by commercial solutions. The Public Safety Communications Research Division incentives may include grant programs, pilot programs, hackathons, or other activities. The Public Safety Communications Research Division may collaborate with SAFECOM and the National Council of Statewide Interoperability Coordinators, the National Public Safety Telecommunications Council, and the FirstNet Authority to identify and develop cybersecurity requirements. Additional collaboration with CISA's Incident Response Team, the National Cybersecurity and Communications Integration Center, and others will help the Public Safety Communications Research Division collect and prioritize known cyber threats for research and development.

Appendix 1: Requirements Matrix

Table A1-1: 6 U.S.C. § 1802 Requirements Cross-referenced with NECP Content

NECP Section	U6 U.S.C. § 572 Requirement Filled
Introduction	6 U.S.C. § 1802(a)-(b) 6 U.S.C. § 1802(c)(7) 6 U.S.C. § 1802(c)(10)
Emergency Communications Ecosystem	6 U.S.C. § 1802(b)(1)-(2) 6 U.S.C. § 1802(c)(3) 6 U.S.C. § 1802(c)(5)
NECP Strategic Goals	6 U.S.C. § 1802(c)
Goal 1: Governance and Leadership	6 U.S.C. § 1802(b) 6 U.S.C. § 1802(c)(5)-(7) 6 U.S.C. § 1802(c)(9)
Goal 2: Planning and Procedures	6 U.S.C. § 1802(c)(1) 6 U.S.C. § 1802(c)(4) 6 U.S.C. § 1802(c)(7)
Goal 3: Training, Exercises, and Evaluations	6 U.S.C. § 1802(a)(1)-(2) 6 U.S.C. § 1802(c)(3) 6 U.S.C. § 1802(c)(5)-(6) 6 U.S.C. § 1802(c)(8)
Goal 4: Communications Coordination	6 U.S.C. § 1802(a)(1)-(2) 6 U.S.C. § 1802(c)(2) 6 U.S.C. § 1802(c)(4)-(6) 6 U.S.C. § 1802(c)(9)
Goal 5: Technology and Infrastructure	6 U.S.C. § 1802(a)(1)-(2) 6 U.S.C. § 1802(c)(1)-(6) 6 U.S.C. § 1802(c)(8)
Goal 6: Cybersecurity	6 U.S.C. § 1802(a)(1)-(2) 6 U.S.C. § 1802(c)(1)-(2) 6 U.S.C. § 1802(c)(8)
Implementation	6 U.S.C. § 1802(c) 6 U.S.C. § 1802(c)(10)
Conclusion	6 U.S.C. § 1802(c) 6 U.S.C. § 1802(c)(8)

This page intentionally left blank.

Appendix 2: Roles and Responsibilities

This appendix provides an overview of the roles and responsibilities of the key public and private stakeholders who are involved in the emergency communications mission and the implementation of the National Emergency Communications Plan (NECP). In addition to emergency responders at all levels of government, this appendix also addresses key private sector and nongovernmental organizations, as well as partnerships and advisory committees, with whom the Federal Government coordinates emergency communications policies, plans, and programs.

All Levels of Government

The responsibility for responding to and managing planned events and unplanned incidents begins at the local level with individuals, first responders, and public officials in the county, city, or town affected by the incident. When emergencies escalate, additional support may be requested from other jurisdictions, states, or even the Federal Government. Operational communications is a core capability for any incident, regardless of size, location, or cause; therefore, each level of government must take the necessary preparedness actions to ensure the capacity to communicate with the emergency response community, affected populations, and other governmental entities.

Local Jurisdictions

Local leaders, emergency managers, and public safety officials prepare their communities to manage incidents and planned events locally. Among their numerous responsibilities, these officials provide strategic guidance, manage resources, develop and implement policies and budgets, implement regional cooperation and planning, and oversee local preparedness efforts to improve emergency management and response capabilities. Several local entities involved in response operations require interoperable, continuous, and secure communications to carry out their missions. This includes public safety disciplines, such as local law enforcement, fire, and emergency medical service personnel who respond to the early stages of an incident and are primarily responsible for the protection and preservation of life, property, evidence, and the environment. In addition, emergency management agencies are also involved with coordination and communications during incidents by disseminating alerts and warnings and operating emergency operations centers, among other key functions. Local public safety answering points and emergency communication centers also play critical roles by serving as key communications and information conduits between the public and emergency responders. Since natural and man-made emergency response efforts generally begin at the local level, coordination among these entities is critical to ensuring effective communications and information sharing when responding to emergencies of all scopes and sizes.

State Agencies

State agencies and officials help coordinate and integrate statewide responders and resources into the local incident command before, during, and after incidents and planned events. States must be prepared to maintain or accelerate the provision of emergency communications resources and services when an incident grows and local capabilities are unable to keep up with demand. Likewise, if a state anticipates that its resources may be exceeded, they must have a process in place to request and integrate federal assistance.

Below is a list of the key statewide officials and governing bodies with responsibility for emergency communications. This list is not intended to be exhaustive, as some states have additional agencies or individuals with whom they interact.[12]

- **Statewide Interoperability Coordinator.** The Statewide Interoperability Coordinator serves as the state's single point of coordination for interoperable communications and implements the Statewide Communication Interoperability Plan, which establishes a vision for interoperability in the state.
- **State Single Point of Contact.** The Single Point of Contact serves as the coordinator for the State and Local Implementation Grant Program and First Responder Network Authority (FirstNet Authority) efforts with respect to the FirstNet Nationwide Public Safety Broadband Network. This person may or may not be the Statewide Interoperability Coordinator.
- **Statewide Interoperability Governing Body or Statewide Interoperability Executive Committee.** The Statewide Interoperability Governing Body or Statewide Interoperability Executive Committee serves as the primary steering group for the statewide interoperability strategy. Its mission is to support the National Council of Statewide Interoperability Coordinators in efforts to improve emergency response communications across the state through enhanced data and voice communications interoperability. Statewide Interoperability Governing Bodies and Statewide Interoperability Executive Committees often include representatives from various jurisdictions and disciplines, as well as subject matter experts.
- **State Emergency Management Agency Director.** The director of the state emergency management agency is responsible for ensuring that the state is prepared to deal with any type of emergency and for coordinating statewide incident response. This includes collaborating with appropriate statewide representatives for critical capabilities, such as emergency communications. The director may also have the responsibility for statewide 911 communications and public alerting.
- **State Information Technology and Security Officials.** A state's or territory's chief information officer, chief technology officer, and chief information security officer manage key information technology and broadband deployment initiatives, including information technology procurement, security, and information technology planning and budgeting.
- **State 911 Administrator.** This individual manages a state's or territory's 911 functions as determined by state legislation. The official title and role of this position may vary by state or territory.

Territories

Similar to states, territorial governments are also responsible for coordinating the emergency communications resources needed to respond to incidents of all types and any scale, determining resource capacity, and ensuring an efficient process for requesting assistance, when necessary. Given that geographical locations often present unique challenges for receiving assistance during times of disaster, it is important for territories to prioritize emergency communications. It is especially critical for territories to build relationships and partnerships among neighboring islands, nearby countries, states, the private sector, nongovernmental organizations, and the Federal Government.

[12] Each state has the ability to designate other officials and offices to oversee aspects of emergency communications and information technology.

Tribal Nations

Tribal nations are geographically dispersed across the United States, and tribe sizes vary significantly, both by enrollment and land area. Federal agencies respect tribal self-government and sovereignty, honor tribal treaties and other rights, and strive to meet the responsibilities that arise from the unique legal relationship between the Federal Government and tribal governments. Communications and emergency services might be handled internally by a tribe; provided by federal, state, or county entities; or handled by any combination thereof. These jurisdictional complexities can greatly complicate emergency response and communications. Many reservations are located in rural areas far from emergency services, which also pose challenges for first responder communications.

Federal Departments and Agencies

The Federal Government has an array of capabilities and resources that can be made available to support emergency response efforts at all levels of government. Federal departments or agencies may function as first responders for incidents and planned events involving primary federal jurisdiction or authorities (e.g., on a military base, a federal facility, or federal lands). Under these circumstances, a federal department or agency becomes the central coordinator of emergency communications activities with state, local, tribal, territorial, and regional partners. Examples include the United States Coast Guard or the Environmental Protection Agency for oil and hazardous materials spills and the United States Forest Service or the Department of the Interior for fires on federal lands.

Emergency Communications Preparedness Center Members

- Department of Agriculture
- Department of Commerce
- Department of Defense
- Department of Energy
- Department of Health & Human Services
- Department of Homeland Security
- Department of the Interior
- Department of Justice
- Department of Labor
- Department of State
- Department of Transportation
- Department of the Treasury
- Federal Communications Commission
- General Services Administration

At the same time, the Federal Government is responsible for ensuring the efficient delivery of federal capabilities for large-scale and catastrophic incidents in support of state, local, tribal, and territorial government efforts, as well as other federal partners. This can include the following communication functions:

- Facilitating federal, state, local, tribal, and territorial planning through funding, technical assistance, and guidance
- Promoting the development of national, regional, and statewide communications plans to address how available federal assets can be incorporated during times of crisis
- Promoting the alignment of federal, state, local, tribal, territorial, and private sector emergency communications plans and preparedness activities to facilitate the development of robust regional communications coordination capabilities
- Supporting federal, state, local, tribal, and territorial operational efforts; providing surge capacity; and coordinating distribution of federal resources to support emergency communications

Private Sector Entities and Nongovernmental Organizations

Private Sector

As the owners and operators of the majority of the Nation's critical infrastructure, private sector entities are responsible for protecting key commercial communications assets, as well as ensuring the resiliency and reliability of communications during day-to-day operations and emergency response and recovery efforts. In addition, commercial communications carriers have a primary role in restoring networks during outages and service failures and supporting reconstitution for emergency response and recovery operations. The communications sector has a history of successfully cooperating both within the sector and with response entities at all levels of government. These relationships help the government and the private sector coordinate joint incident response activities, share and analyze infrastructure information, and coordinate standards development and priority service technologies.

Private Sector Partnerships

"Update national strategies (such as the National Response Framework and the NECP) and initiatives to account for advanced [Next Generation Network] communications capabilities, such as the [FirstNet] Nationwide Public Safety Broadband Network, and to reflect the evolving communications environment."

- National Security Telecommunications Advisory Committee Report to the President on the National Security and Emergency Preparedness Implications of a [FirstNet] Nationwide Public Safety Broadband Network.

The private sector's extensive experience protecting, restoring, and reconstituting the communications infrastructure will be particularly important as the Nation plans and prepares for the adoption, migration, and use of emerging technologies, including the continued deployment of the FirstNet Nationwide Public Safety Broadband Network. It provides insight on how to address network vulnerabilities so that emergency communications are reliable and resilient during times of crisis.

Depending on the type of incident and its scale, other private sector entities may also have a role supporting, facilitating, or using communications during emergencies, as well as providing services and networks for the government to alert the public. For example, key private sector partners—including privately owned transportation and transit, telecommunications, utilities, financial institutions, hospitals, and other health regulated facilities—may need to establish and maintain a direct line of communication between their organization and emergency response officials.

Nongovernmental Organizations

Nongovernmental organizations can play vital roles during emergency response and recovery operations, as they have the capability to deliver specialized services that support core capabilities, including operational communications.[13] Nongovernmental organizations include voluntary and non-profit organizations that provide shelter, food, and other essential support services and disaster relief.[14] As technology evolves, nongovernmental organizations are also implementing new ways to facilitate communications and information sharing during emergencies.

Nongovernmental Organization Communications during Response Operations

The American Red Cross has established a digital operations center in Washington, D.C., that enables the organization to more effectively understand and anticipate disaster needs in order to deploy assistance more efficiently. The center has the capability to monitor, respond to, and analyze social media platforms, share timely information, coordinate with other emergency response entities, and allocate resources accordingly. The American Red Cross has developed a training program to leverage digital volunteers that can be called upon to scale up digital operations for emergency situations such as Hurricanes Maria, Harvey, and Florence.

Individuals and Volunteer Organizations

As discussed in Section 2.0 of the NECP, the public and volunteer groups play an increasingly important role in emergency communications. Emergencies are often first reported to authorities by members of the public seeking assistance, and—more than ever before—the public is encouraged to alert the government to potentially dangerous or suspicious activities or update officials on the aftermath of an incident. For example, the Department of Homeland Security's (DHS) "If You See Something, Say Something®" campaign emphasizes the importance of reporting suspicious activity to the proper local law enforcement authorities.

Likewise, volunteer organizations such as auxiliary communications volunteers play key roles in emergency communications and preparedness. Volunteer emergency communications operators and groups using amateur radio have been providing backup communications to event planners, public safety officials, and emergency managers at all levels of government for nearly 100 years. Often, amateur radio services have been used when other forms of communications have failed or have been disrupted. Today, nearly all the states and territories have incorporated some level of participation by amateur radio auxiliary communication operators into their Tactical Interoperable Communications Plans and Statewide Communication Interoperability Plans, allowing them to quickly integrate the operators into response efforts, which can strengthen communications and operations during incidents and planned events of any scale.

[13] For a list of all core capabilities, refer to the National Preparedness Goal, www.fema.gov/ppd8
[14] The Federal Emergency Management Agency. National Response Framework, June 2016, pg. 9, https://www.fema.gov/media-library-data/1466014682982-9bcf8245ba4c60c120aa915abe74e15d/National_Response_Framework3rd.pdf

Partnership and Advisory Groups

Partnership groups are key mechanisms for successful implementation of the NECP and execution of the national emergency communications mission. They provide best practices and subject matter expertise to the government and allow emergency response stakeholders to cultivate working relationships and help shape strategic and operational plans to improve emergency communications. With the changes in the Emergency Communications Ecosystem, as noted in Section 2.0 of the NECP, the pool of partnerships and their roles and responsibilities for supporting emergency communications continues to evolve and expand. The following list includes key partnership organizations and advisory bodies:

- **Canada – United States Communications Interoperability Working Group.** The Canada – United States Communications Interoperability Working Group is a joint effort between Canada and the United States. It is co-chaired by Public Safety Canada and DHS CISA. The Interoperability Working Group's goal is to support each country's national interoperability strategy and work to resolve bilateral issues of common interest concerning cross-border communications and information exchange.
- **Communications Security, Reliability and Interoperability Council.** The Communications Security, Reliability and Interoperability Council is an advisory committee that provides recommendations to the Federal Communications Commission to ensure, among other things, optimal security and reliability of communications systems, including telecommunications, media, and public safety.
- **Critical Infrastructure Partnership Advisory Council.** The Critical Infrastructure Partnership Advisory Council is a DHS program established to facilitate effective coordination of critical infrastructure activities among the Federal Government; the private sector; and state, local, tribal, and territorial governments.
- **Emergency Communications Preparedness Center.** As the federal interagency focal point for interoperable and operable emergency communications coordination, the Emergency Communications Preparedness Center's mission is to improve emergency communications collaboration across the Federal Government and align initiatives with national goals, policy, and guidance. The 14 federal departments and agencies that comprise the Emergency Communications Preparedness Center represent the Federal Government's broad role in emergency communications, including planning, policy, operations, grants, and technical assistance.
- **Federal Partnership for Interoperable Communications.** Serves as a coordination and advisory body to address technical and operational wireless issues related to interoperability within the public safety emergency communications community, interfacing with voluntary representatives from federal, state, local, territorial, and tribal organizations. The Federal Partnership for Interoperable Communications includes several subcommittees and focus groups working on encryption, the inter-radio frequency subsystem interface, the console subsystem interface, governance-based interoperability, and other pertinent topics.
- **National Council of Statewide Interoperability Coordinators.** Comprised of all Statewide Interoperability Coordinators, the National Council of Statewide Interoperability Coordinators assists Statewide Interoperability Coordinators with promoting the critical importance of

interoperable communications and the sharing of best practices to ensure the highest level of interoperable communications across the Nation.

- **National Public Safety Telecommunications Council.** Composed of state and local public safety representatives, the National Public Safety Telecommunications Council is a federation of national public safety leadership organizations dedicated to improving emergency response communications and interoperability through collaborative leadership.
- **National Security and Emergency Preparedness Communications Executive Committee.** Executive Order 13618, *Assignment of National Security and Emergency Preparedness Communications Functions*, established the National Security and Emergency Preparedness Communications Executive Committee, which is an interagency forum that addresses national security and emergency preparedness communication matters through policy recommendations on enhancing the survivability, resilience, and future architecture of national security and emergency preparedness communications.
- **National Security Telecommunications Advisory Committee.** The President's National Security Telecommunications Advisory Committee is composed of private sector executives who represent major communications and network service providers and information technology, finance, and aerospace companies. Through DHS, the National Security Telecommunications Advisory Committee provides private sector-based analyses and recommendations to the President and the Executive Branch on policy and enhancements to national security and emergency preparedness communications information and communications services, as well as advice regarding the feasibility of implementing specific measures to improve the telecommunications aspects of the national security posture.
- **Public Safety Advisory Committee.** The Public Safety Advisory Committee is a standing advisory committee that assists the First Responder Network Authority in carrying out its duties and responsibilities. The Public Safety Advisory Committee is comprised of over 40 representatives from various public safety organizations (as well as the federal, state, territorial, tribal, and local governments), many of which also participate in SAFECOM.
- **Regional Emergency Communications Coordination Working Group.** The Regional Emergency Communications Coordination Working Groups serve as the single coordination points for emergency communications at the regional level. A Regional Emergency Communications Coordination Working Group has been established in each of the 10 Federal Emergency Management Agency regions. Each Regional Emergency Communications Coordination Working Group has a unique membership based on regional government structure and processes.
- **SAFECOM.** SAFECOM is an emergency communications program at DHS. As a stakeholder-driven program, SAFECOM is led by an Executive Committee, in support of the overall membership, which is primarily composed of state and local emergency responders and intergovernmental and national public safety communications associations. SAFECOM regularly convenes to discuss interoperability and emergency communications and to provide input on challenges, needs, and best practices of emergency responders. CISA develops policy, guidance, and future initiatives by drawing on the expertise of the Executive Committee.

- **Southwest Border Communications Working Group.** The Southwest Border Communications Working Group is a diverse, multi-disciplinary group that supports federal, state, local and territorial agency efforts in the Southwest Border Region (Arizona, California, New Mexico, and Texas) to establish, expand, and maintain operable and interoperable public safety communications. The working group's purpose is to expand and enhance the quality of critical public safety communications while effectively and collaboratively identifying, documenting, and facilitating the sharing of scarce regional infrastructure resources, spectrum, and services. This effort includes close coordination with the FirstNet Authority as it develops and deploys a nationwide broadband network that will enhance public safety agencies' data communications capabilities.

Appendix 3: SAFECOM Interoperability Continuum

Developed with practitioner input from the Department of Homeland Security's (DHS) SAFECOM program, the Interoperability Continuum is designed to assist emergency response agencies and policy makers to plan and implement interoperability solutions for data and voice communications. This tool identifies the five critical success elements that must be addressed to achieve a sophisticated interoperability solution: governance, standard operating procedures, technology, training and exercises, and usage of interoperable communications (Figure A3-1). The Interoperability Continuum can be used by jurisdictions to track progress in strengthening interoperable communications. In addition, the DHS Cybersecurity and Infrastructure Security Agency (CISA) has used the Interoperability Continuum to develop the priorities and measure the goals of the National Emergency Communications Plan (NECP). For more information, see Implementing the NECP.

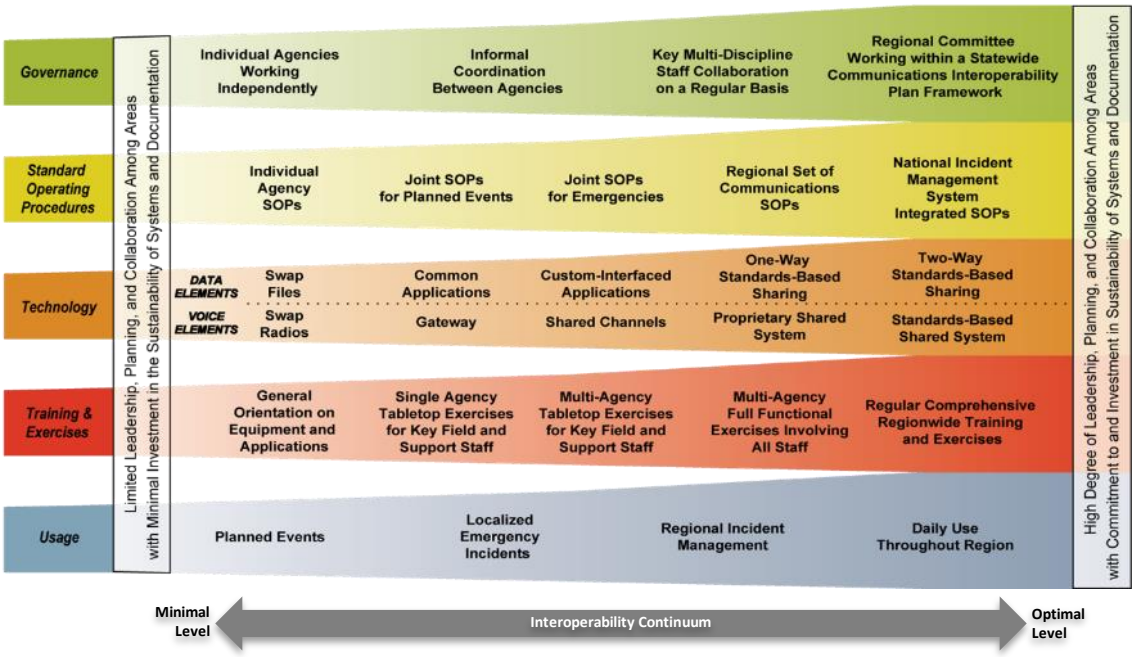


Figure A3-1. SAFECOM Interoperability Continuum

Interoperability is a multi-dimensional challenge. To gain a realistic picture of a region's interoperability, progress in each of the five interdependent elements must be considered. For example, when a region procures new equipment, that region should plan and conduct training and exercises to maximize the use of that equipment. Optimal-level interoperability is contingent upon individual agency and jurisdictional needs. The Continuum is designed as a guide for jurisdictions that are pursuing a new interoperability solution based on changing needs or additional resources; it is an evolving tool that supports national preparedness doctrine including, but not limited to, the National Incident Management System, the National Response Framework, and the NECP. To maximize the Interoperability Continuum's value to the emergency response community, SAFECOM will regularly update the tool through a consensus process involving practitioners, technical experts, and representatives from federal, state, tribal, territorial, regional, and local agencies.

This page intentionally left blank.

Appendix 4: Source Documents and References

This appendix lists the key source documents, authorities, and references that the Cybersecurity and Infrastructure Security Agency (CISA) used to inform and shape the concepts, goals, and objectives of the National Emergency Communications Plan (NECP). This list is not exhaustive; rather, it highlights the primary source documents that were developed since the NECP was published in 2014.

Statutory Authorities

The following list includes key authorities that guide the development, implementation, and management of the NECP. For example, *Title XVIII of the Department of Homeland Security Appropriations Act of 2007* impacts the NECP directly by requiring CISA to periodically update the plan.[15] In addition, related statutes pertaining to emergency communications nationwide also indirectly help to guide NECP improvements and revisions. This list identifies the foundational statutes on which emergency communications functions are executed.

1. *Communications Act of 1934, Pub. L. No. 73-416) (1934), as amended by the Telecommunications Act of 1996, Pub. L. No 104-104 (1996)*
2. *Robert T. Stafford Disaster Relief and Emergency Assistance Act ("Stafford Act"), Pub. L. No. (as amended 1988)*
3. *Homeland Security Act of 2002, Pub. L. No. 107-296 (as amended 2002)*
4. *Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458 (codified as amended at 6 U.S.C. § 194(a)(1) (2004))*
5. *Security and Accountability for Every Port Act of 2006, Pub. L. No. 109–347 (codified at 42 U.S.C. § 1201 (2006))*
6. *Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53 (codified as amended at 6 U.S.C. § 572(c)(10))*
7. *Middle-Class Tax Relief and Jobs Creation Act of 2012, Pub. L. No. 112-96 (codified at 47 U.S.C. § 1426 (2012))*
8. *Next Generation 911 Advancement Act of 2012, Pub. L. No. (P.L. 112-96) (codified as amended at 47 U.S.C. 942 (2012))*

Administrative and Executive Authorities

Below are related presidential directives and executive orders that affect NECP development and implementation processes. For example, these authorities set national policy and provide executive direction in areas closely related to emergency communications, including national preparedness, domestic incident management, critical infrastructure resilience, cybersecurity, and continuity of government operations. As such, NECP concepts and strategies align with these authorities, are shaped by them, or both.

1. *Homeland Security Presidential Directive 5, Management of Domestic Incident* (2003)

[15] 6 U.S.C. § 572. NECP (2007)

2. *Homeland Security Presidential Directive 7, Critical Infrastructure Identification, Prioritization, and Protection* (2003)
3. *Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors* (2004)
4. *Homeland Security Presidential Policy Directive 40, National Continuity Policy, July 15, 2016*
5. *National Security Decision Directive 97, National Security Telecommunications Policy* (1983)
6. *National Security Presidential Directive 39, United States Space-Based Position, Navigation, and Timing Policy* (2004)
7. *Presidential Policy Directive 8, National Preparedness* (2011)
8. *Presidential Policy Directive 21, Critical Infrastructure Security and Resilience* (2013)
9. *Presidential Decision Directive 4, National Space Policy* (2007)
10. *Presidential Decision Directive 41, U.S. Cyber Incident Coordination* (2016)
11. *Executive Order 13175, Consultation and Coordination with Indian Tribal* (2000)
12. *Executive Order 13407, Integrated Public Alert and Warning System* (2006)
13. *Executive Order 13618, Assignment of National Security and Emergency Preparedness Communications Functions* (2012)
14. *Executive Order 13616, Accelerating Broadband Infrastructure Deployment* (2012)
15. *Executive Order 13636, Improving Critical Infrastructure Cybersecurity* (2013)

Related References

The following homeland security policies, plans, and doctrine influence the NECP updates and implementation lifecycle.

1. *National Preparedness System* (2011)
2. *National Infrastructure Protection Plan* – National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience (2013)
3. *National Preparedness Goal, Second Edition* (2015)
4. *National Response Framework, Third Edition* (2016)
5. *Response Federal Interagency Operational Plans, Second Edition* (2016)
6. *National Preparedness Report* (2017)
7. *National Incident Management System, Third Edition* (2017)

Federal Departments and Agencies

1. U.S. Department of Homeland Security. *DHS Cybersecurity Services Catalog for State, Local, Tribal, and Territorial Governments. 2018*. https://www.us-cert.gov/sites/default/files/c3vp/sltt/SLTT_Hands_On_Support.pdf
2. U.S. Department of Homeland Security. CISA. *Fiscal Year 2018 SAFECOM Guidance on Emergency Communications Grants.* 2018.

https://www.cisa.gov/sites/default/files/publications/FY2018_SAFECOM_Guidance_FINAL_508C_060518.pdf

3. U.S. Department of Homeland Security. Federal Emergency Management Agency. *Comprehensive Preparedness Guide 201: Threat and Hazard Identification and Risk Assessment and Stakeholder Preparedness Review Guide, Third Edition.* 2018. https://www.fema.gov/media-library/assets/documents/165308
4. U.S. Department of Homeland Security. Federal Emergency Management Agency. *National Incident Management System*. 2017. https://www.fema.gov/national-incident-management-system
5. U.S. Department of Homeland Security. Federal Emergency Management Agency. *2017 National Preparedness Report*. 2017. https://www.fema.gov/national-preparedness-report
6. U.S. Department of Homeland Security. Federal Emergency Management Agency. *National Response Framework, Third Edition*. https://www.fema.gov/media-library/assets/documents/117791
7. Federal Communications Commission. *Task Force on Optimal Public Safety Answering Point Architecture*. 2015. https://www.fcc.gov/about-fcc/advisory-committees/general/task-force-optimal-public-safety-answering-point
8. National 911 Program Office. *Guidelines for State Next Generation 911 Legislative Language*. 2018. https://www.911.gov/pdf/Guidelines_for_State_NG911_Legislative_Language.pdf
9. National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity*. 2018. https://www.nist.gov/cyberframework
10. National Institute of Standards and Technology. Project 25 Compliance Assessment Program, https://www.nist.gov/ctl/pscr/newsroom/press/p25-cap

Congressional Panels, Testimonies, and Reports

1. U.S. House of Representatives. Committee on Homeland Security Subcommittee on Emergency Preparedness, Response, and Communications. *Written Testimony of Rear Admiral Ronald Hewitt, USCG (Retired) Assistant Director for Emergency Communications, CISA*. October 12, 2017. https://docs.house.gov/meetings/HM/HM12/20171012/106503/HHRG-115-HM12-Wstate-HewittR-20171012.pdf

National Associations, Advisory Boards and Groups, Other Research Reports

1. 2017 Joint Meeting of the Major Cities Chiefs Association's Technology and FirstNet: Workshop on Law Enforcement Priorities and Recommendations for FirstNet. March 2017. https://www.majorcitieschiefs.com/pdf/news/mcca__firstnet_announcement_press_release_3.30.2017.pdf
2. National Emergency Management Association. *2018 Biennial Report*. 2018. https://files.constantcontact.com/4ac009d3101/abaaaf91-dae2-442d-9338-06e130151c4a.pdf
3. Via Satellite. *First Responder's Guide to Satellite Communications*. 2018. https://www.satellitetoday.com/first-responders-guide-to-satellite-communications/

4. National Public Safety Telecommunications Council. *NPSTC Report: Best Practices for Public Safety Interoperable Communications*. 2018.
5. Hollywood, John S., Dulani Woods, Andrew Lauland, Sean E. Goodison, Thomas J. Wilson, and Brian A. Jackson. *Using Future Broadband Communications Technologies to Strengthen Law Enforcement*. Santa Monica, CA: RAND Corporation, 2016. https://www.rand.org/pubs/research_reports/RR1462.html

Appendix 5: Glossary

After-Action Report
A professional document formulated in partnership with participants in a process. Evaluators, sponsoring agencies, and key participants from government agencies participate in the formulation of the after-action report. It furnishes a historical record of findings and it forms the foundation for refinements to plans, policies, procedures, training, equipment, and overall preparedness of an entity. The report depicts the process, preliminary observations, and major issues, and makes recommendations for improvements.

Alerts, Warnings, and Notifications
The alerting ecosystem consists of multiple systems that originators of an alert can use to reach the public with alert and warning information; it also includes diverse channels of message delivery, distributed sensing devices, and feedback mechanisms. Alerting ecosystem components include alerts and warnings from alerting authorities to the public, coordination between alerting authorities and other governmental entities, public information sharing to alerting authorities, and public information exchange between community members.

All Hazards Incident Dispatch Team
Specially trained communications personnel who are certified in tactical, wildland, and urban-interference incidents. The Incident Dispatch Team responds to large-scale events and incidents and works with the varying levels of communications at the scene.

Applications
A set of features and a user interface that may be realized by fixed or mobile devices. User services are logical building blocks of application-layer functionality.

Agreements
Formal mechanisms to govern interagency coordination and the use of interoperable emergency communications solutions.

Assessment
Used to provide a basis for decision making, assessment is the process of acquiring, collecting, processing, examining, analyzing, evaluating, monitoring, and interpreting the data, information, evidence, objects, measurements, images, and sound, among others, whether tangible or intangible.

Amateur Radio Service
A radio communication service for the purpose of self-training, intercommunication, and technical investigations carried out by amateurs, who are duly authorized persons interested in radio technique solely with a personal aim and without pecuniary interest.

Auxiliary Communications
Backup emergency radio communications provided by volunteers who support public safety and emergency response professionals and their agencies.

Big Data
The analysis of datasets that are too massive, too complex, or too disparate to be handled by traditional data processing methods. For example, the New York City Fire Department utilizes a Risk-Based Inspection System to score buildings' fire risk and prioritize those that need inspection most urgently. Big Data also includes predictive algorithms that give advance notice for disasters, both natural and man-made; management of after-action reports within the context of larger data sets; and analytic engines that reveal important correlations that can improve management efficiency for public safety, reduce overhead costs and manpower requirements, and even improve responder health and safety.

Broadband
High-speed internet that allows users to access the internet and internet-related services at significantly higher speeds using long-term evolution technology. Broadband and long-term evolution allow users to access the next evolution of commercial broadband wireless communications technology—which was developed to address the demand for high-speed, data-intensive communications—such as situational awareness, advanced analytics, database queries, and video applications. Transmission is digital, meaning that text, images, and sound are transmitted as bits of data. The transmission technologies that make broadband possible move these bits much more quickly than traditional telephone or wireless connections.

Capital Investments
Equipment and other one-time costs.

Common Alerting Protocol
The Common Alerting Protocol is a digital format for exchanging emergency alerts allowing consistent alert messages to be disseminated simultaneously over many different communications systems.

Communications Coordinator
Serves as a point of contact and is responsible for maintaining contact with local agencies, collecting information about local resources to aid the Communications Unit Leader, and helping with tasks such as assigning equipment and frequencies and following up on and keeping track of the status of orders. The Communications Coordinator determines the extent and availability of communications coordination possible for a given incident.

Communications Duty Officer
Similar to the Communications Coordinator, serves as a point of contact and is responsible for maintaining contact with local agencies and collecting information about local resources to aid the Communications Unit Leader.

Communications Unit Leader
The Communications Unit Leader heads the communications unit and is responsible for integrating communications. The Communications Unit Leader designs, orders, manages, and ensures the installation and maintenance of all communications systems. The Communications Unit Leader must be familiar with Incident Command Systems and local response systems to support incident personnel efforts.

Continuity
Ability to provide and maintain acceptable levels of communications during disruptions in operations.

Continuity of Communications
The ability of emergency response agencies to maintain communications capabilities when primary infrastructure is damaged or destroyed.

Core Capabilities
Distinct critical elements necessary to achieve the National Preparedness Goal.

Critical Infrastructure
Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or medical, or safety, or any combination of those matters. (*Source: 2013 National Infrastructure Protection Plan*)

Cross-Discipline
Involving emergency response providers from different disciplines (e.g., police, fire, emergency medical services).

Cybersecurity
The prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability. Includes the protection and restoration (when needed) of information networks and wireline, wireless, satellite, public safety answering points, and 911 communications systems and control systems. (*Source: 2013 National Infrastructure Protection Plan: Partnering for Critical Infrastructure Security and Resilience*)

Cybersecurity Risks
Occur when a cybersecurity threat exploits a vulnerability, increasing the likelihood of or leading to an undesired event that has a negative consequence on the desired state of the network.

Cybersecurity Threats
Anything that has the potential to harm the system and are produced by "threat actors" who possess capabilities to carry out an attack.

Day-to-Day Situations
Situations within the general normal structure for an organization, including routine operations.

Decision-Making Groups
A group or governing body with a published agreement that designates its authority, mission, and responsibilities.

Emergency Communications
The means and methods for exchanging communications and information necessary for successful incident management.

Emergency Communications Center/Public Safety Answering Point
The terms defining the Nation's 911 and public safety communications centers have matured over time. The NECP references the term "emergency communications center/public safety answering point." For purposes of this document, "emergency communications center/public safety answering point" is meant to encompass the following definitions:

- Public safety answering point: a center "where 911 requests are answered, evaluated, and processed to determine whether dispatch of field responders is needed, and in what form." [*Task Force on Optimal Public Safety Answering Point*]

- Emergency communication center: "a facility with capabilities that include intelligence collection and monitoring, 911 multimedia traffic processing, full-scale dispatch, and incident capabilities." [*Association of Public-Safety Communications Officials Project 43*]
- 911 communication center: "a facility that is designated by a governmental authority to perform the functions of a Public Safety Answering Point and perform one or more of the following functions: (1) process and analyze 911 Requests for Emergency Assistance and other gathered information, (2) dispatch appropriate Emergency Response Providers, (3) transfer or exchange 911 Requests for Emergency Assistance and other gathered information with other Emergency Communications Centers and Emergency Response Providers, (4) analyze any communications received from Emergency Response Providers, and (5) perform incident command functions." [*National Emergency Number Association*]
- Public safety communications center: "a public safety entity where 911 or other emergency calls for service are processed and public safety resources are dispatched." [*Association of Public-Safety Communications Officials / National Emergency Number Association American National Standards Institute 107.1-2015*]

The NECP uses the "emergency communications center/public safety answering point" term to better encompass the nature of the Nation's 911 and public safety communications centers. The processes and procedures to transition to Next Generation 911 do not depend on these terms; therefore, NECP recommendations are not impacted by the use of any specific term.

Emergency Communications Ecosystem

A concept referring to the various functions and people that exchange information prior to, during, and after incidents and planned events.

Emergency Management Assistance Compact

A congressionally ratified mutual aid compact that legally establishes a national system to facilitate resources across state lines during an emergency or disaster.

Emergency Response Providers

The Homeland Security Act of 2002 defines emergency response providers as federal, state, and local governmental and nongovernmental emergency public safety, fire, law enforcement, emergency response, emergency medical (including hospital emergency facilities), and related personnel, agencies, and authorities.

Emergency Support Functions

Used by the Federal Government and many state governments as the primary mechanism at the operational level to organize and provide assistance. Emergency Support Functions align categories of resources and provide strategic objectives for their use. Emergency Support Functions utilize standardized resource management concepts such as typing, inventorying, and tracking to facilitate the dispatch, deployment, and recovery of resources before, during, and after an incident.

Encryption

Method of mitigating threats from the potential compromise of personal or sensitive data by encoding information in such a way that only authorized parties can access it.

Exercises
Instruments to train for, assess, practice, and improve performance in prevention, protection, mitigation, response, and recovery capabilities in a risk-free environment. Exercises can be used for testing and validating policies, plans, procedures, training, equipment, and interagency agreements; clarifying and training personnel in roles and responsibilities; improving interagency coordination and communications; improving individual performance; identifying gaps in resources; and identifying opportunities for improvement.

First Responder Network Authority (FirstNet Authority)
An independent authority within the National Telecommunications and Information Administration that is responsible for ensuring the building, deployment, and operation of the first high-speed Nationwide Public Safety Broadband Network.

First Responders
See "emergency response provider." (The Implementing the 9/11 Commission Recommendations Act of 2007 states that the term "first responder" shall have the same meaning as the term "emergency response provider," which is defined in the Homeland Security Act of 2002.)

Government Emergency Telecommunications Service
Service that provides national security and emergency preparedness personnel with priority access and prioritized processing in the local and long-distance segments of the Public Switched Telephone Network, greatly increasing the probability of call completion. Government Emergency Telecommunications Service is intended to be used in an emergency or crisis situation when the Public Switched Telephone Network is congested and the probability of completing a normal call is reduced. https://www.cisa.gov/cisa/government-emergency-telecommunications-service-gets

Governance
Relates to consistent management, cohesive policies, guidance, processes, and decision-rights for a given area of responsibility.

Homeland Security Exercise and Evaluation Program
Provides a set of guiding principles for exercise programs, as well as a common approach to exercise program management, design and development, conduct, evaluation, and improvement planning. Homeland Security Exercise and Evaluation Program exercise and evaluation doctrine is flexible, adaptable, and is for use by stakeholders across the whole community and is applicable for exercises across all mission areas – prevention, protection, mitigation, response, and recovery.

Incident Action Plan
An oral or written plan containing general objectives reflecting the overall strategy for managing an incident. It may include the identification of operational resources and assignments. It may also include attachments that provide direction and important information for management of the incident during one or more operational periods.

Incident Communications Center Manager
Manages an Incident Communications Center when the Communications Unit Leader's span of control would be exceeded by the complexity of the incident. The Incident Communications Center Manager serves primarily to supervise radio operators and manage the increased complexity of an Incident Communications Center during large incidents.

Incident Communications Center
An established location close to an Incident Command Post from which coordination, communications, and support of incident management activities is directed.

Incident Command System
A standardized on-scene emergency management construct specifically designed to provide for the adoption of an integrated organizational structure that reflects the complexity and demands of single or multiple incidents, without being hindered by jurisdictional boundaries. The Incident Command System is the combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure that is designed to aid in the management of resources during incidents. It is used for all kinds of emergencies and is applicable to incidents ranging from small to large and complex. The incident command system is used by various jurisdictions and functional agencies, both public and private, to organize field-level incident management operations.

Information Sharing Environment
Broadly refers to the people, projects, systems, and agencies that enable responsible information sharing for national security.

Information Technology Service Unit Leader
Responsible for coordinating with the Communications Leader and Incident Commander Staff to determine information technology resource requirements to support incident objectives such as developing an Information Management Plan (manage data sharing); determining and ordering needed personnel, equipment, and services; and supervising information technology and the Communications Help Desk.

Integrated Public Alert and Warning System (IPAWS)
Federal Emergency Management Agency built IPAWS to ensure that under all conditions the President of the United States can alert and warn the American people. Federal, state, local, tribal, and territorial authorities also have the opportunity to use IPAWS to send alerts and warnings within their jurisdictions. IPAWS improves alert and warning capabilities by allowing authorities to deliver alerts simultaneously through multiple communications devices reaching as many people as possible to save lives and protect property.

International/Cross-Border Entities
Foreign organizations (e.g., Canadian or Mexican organizations).

Interoperability
Ability of emergency response providers and relevant government officials to communicate across jurisdictions, disciplines, and levels of government as needed and as authorized.

Interoperability Solutions
Any method, process, or system used to enable interoperability (e.g., radio swaps, channel or console cross-patching, shared system or channels).

Internet of Things
The Internet of Things is the network of physical devices and connectivity that enables objects to connect to one another, to the internet, and exchange data amongst themselves. Internet of Things can benefit public safety by providing ubiquitous network connectivity, enhanced situational awareness, process optimization, and real time response/control of autonomous systems. However, integrating Internet of Things into a public safety operational framework also poses some concerns regarding cybersecurity, scale, network congestion, interoperability, human impacts, and policy over Internet of Things provisioning and priority and privacy of data.

Jurisdiction
A range or sphere of authority. Public safety agencies have jurisdiction at an incident related to their legal responsibilities and authority. Jurisdictional authority at an incident can be political or geographical (e.g., federal, state, tribal, territorial, regional, and local boundary lines) or functional (e.g., law enforcement, public health, medical).

Land Mobile Radio Systems
Terrestrially based wireless narrowband communications systems commonly used by federal, state, tribal, territorial, and local emergency responders; public works companies; and even the military to support voice and low-speed data communications.

Lifecycle Planning
The process of designing, implementing, supporting, and maintaining a land mobile radio or mobile data-based public safety communications system. Enables practitioners to better forecast long-term funding requirements and helps to set the framework for establishing and maintaining a public safety system.

Mission Areas
Groups of core capabilities, including prevention, protection, mitigation, response, and recovery.

Multi-jurisdictional
Involving agencies from different jurisdictions (e.g., across state, county, or regional boundaries).

Mutual Aid Agreement or Assistance Agreement
Written or oral agreement between and among agencies, organizations, or jurisdictions that provides a mechanism to quickly obtain emergency assistance in the form of personnel, equipment, materials, and other associated services. The primary objective is to facilitate rapid, short-term deployment of emergency support prior to, during, or after an incident.

National Emergency Communications Plan (NECP)
The Homeland Security Act of 2002, as amended, requires DHS to develop the NECP; the NECP serves as the Nation's strategic plan for improving emergency response communications and efforts in the United States.

National Incident Management System
Provides a systematic, proactive approach and template to guide departments and agencies at all levels of government, nongovernmental organizations, and the private sector to work seamlessly to prevent, protect against, respond to, recover from, and mitigate the effects of incidents, regardless of cause, size, location, or complexity, in order to reduce the loss of life or property and harm to the environment.

National Preparedness Goal
The cornerstone for the implementation of Presidential Policy Directive 8, it establishes the capabilities and outcomes for the Nation to accomplish across five mission areas (prevention, protection, mitigation, response, and recovery) in order to be secure and resilient. The goal establishes distinct core capabilities and corresponding target elements for each mission area.

Nationwide Public Safety Broadband Network
A dedicated, wireless, interoperable, communications long-term evolution-based network (consisting of a core network and radio access network) that allows public safety to receive and share critical information with their counterparts across the Nation.

National Response Framework
A guide to how the Nation responds to all types of disasters and emergencies. It describes specific authorities and best practices for managing incidents that range from the serious but purely local to large-scale terrorist attacks or catastrophic natural disasters.

National Security and Emergency Preparedness Communications Functions
The ability of the Federal Government to communicate at all times and under all circumstances to carry out its most critical and time-sensitive missions. This includes the survivable, resilient, enduring, and effective communications, both domestic and international, that are essential to enable the executive branch to communicate within itself and with the legislative and judicial branches; state, tribal, territorial, and local governments; private sector entities; and the public, allies, and other nations.

Nongovernmental Organizations
As noted in the National Response Framework, these include voluntary, racial and ethnic, faith-based, veteran-based, and nonprofit organizations that provide sheltering, emergency food supplies, and other essential support services. Nongovernmental organizations are inherently independent and committed to specific interests and values.

Nongovernmental Organizations/Private Sector
Non-profit or for-profit organizations participating in public safety/emergency communications planning, use or reconstitution (e.g., nongovernmental organizations, utilities, communication service providers, equipment operators, transportation, food distribution, Volunteer Organizations Active in Disasters).

Operability
Ability to provide and maintain reliable communications functionality throughout the area of responsibility.

Operating Environment
For the purposes of the NECP, this refers to the people, processes, policies, and technologies for emergency communications.

Other Disciplines
Personnel with another organization of a different discipline (e.g., law enforcement, fire) within the same jurisdiction.

Out-of-the-Ordinary Situations
Situations that may stretch and/or overwhelm the abilities of an organization.

Personnel
Individuals responsible for communications installations, operations, and maintenance.

Position Task Book
Primary tool for observing and evaluating the performance of Incident Command System trainees. They allow documentation of a trainee's ability to perform each task, as prescribed by position.

Priority Telecommunications Service
Implements policy, assigns responsibilities, and establishes procedures for the Telecommunications Service Priority Program. Authorizes priority services for domestic telecommunications services (e.g., Government Emergency Telecommunications Service and Wireless Priority Service).

Private Sector Entity
Per the National Response Framework, private sector entities include large, medium, and small businesses; commercial, private cultural, and educational institutions; and industry, as well as public-private partnerships that have been established specifically for emergency management purposes.

Project 25
A suite of standards for digital radio communications for use by federal, state/province and local public safety agencies in North America to enable them to communicate with other agencies and mutual aid response teams in emergencies. In this regard, Project 25 fills the same role as the European Terrestrial Trunked Radio protocol, but the two are not interoperable.

Protective/Restorative Measures
Protective measures decrease the likelihood that a threat will affect the network, while restorative measures, such as the Telecommunications Service Priority, enable rapid restoration if services are damaged or destroyed.

Public Safety Entity
An entity that provides public safety services that include services provided by emergency response providers, as defined in the Homeland Security Act of 2002.

Public Safety
Refers to the welfare and protection of the general public.

Public Safety/Emergency Communications
Capabilities needed to transmit/receive information during public safety incidents (e.g., natural disasters, acts of terrorism, other man-made events) and planned events.

Public Safety Services
Includes services defined in the Communications Act of 1934 as those with the sole or principal purpose of which is to protect the safety of life, health, or property; that are provided—by state or local government entities; or by nongovernmental organizations that are authorized by a governmental entity whose primary mission is the provision of such services; and that are not made commercially available to the public by the provider. Also includes services provided by emergency response providers, as defined in Section 2 of the Homeland Security Act of 2002.

Public Safety Answering Point
A facility that has been designated to receive 911 calls and route them to emergency services personnel. A public safety answering point may act as a dispatch center. Public safety answering point is often used with the term emergency communication center.

Reliability
Achieved in public safety land mobile radio systems through equipment redundancy and minimizing single points of failures through careful system design. System operators stock spare parts and, in some cases, transportable backup systems to restore system failures that do occur. Reliability must be considered at the earliest stages of system design.

Redundancy
Additional or duplicate communications assets share the load or provide back-up to the primary asset.

Resources
Personnel and major items of equipment, supplies, and facilities available or potentially available for assignment to incident operations and for which status is maintained. Resources are described by kind and type and may be used in operational support or supervisory capacities at an incident or at an Emergency Operations Center.

Route Diversity
Communications routing between two points over more than one geographic or physical path with no common points.

Social Media
Refers to the means of interactions among people in which they create, share, or exchange information and ideas in virtual communities and networks.

Standard Operating Procedures
Generally refers to a reference document or an operations manual that provides the purpose, authorities, duration, and details for the preferred method of performing a single function or a number of interrelated functions in a uniform manner.

Stakeholder Preparedness Review
Required by several DHS grants, the Threat and Hazard Identification and Risk Assessment process helps communities understand threats and hazards and their varying impacts. The Threat and Hazard Identification and Risk Assessment process results in community-informed capability targets and resource requirements necessary to address anticipated and unanticipated risks.

Strategic Planning
A planning process that establishes organizational goals and identifies, scopes, and establishes requirements for the provisioning of capabilities and resources to achieve them.

Statewide Communication Interoperability Plan
Stakeholder-driven, multi-jurisdictional, and multi-disciplinary statewide plans that outline and define the current and future vision for communications interoperability within the state or territory. The Statewide Communication Interoperability Plan is a critical strategic planning tool to help states prioritize resources, establish and strengthen governance, identify future technology investments, and address interoperability gaps.

Statewide Interoperability Coordinator
Serves as the state's single point of coordination for interoperable communications and implements the Statewide Communication Interoperability Plan.

Statewide Interoperability Governing Bodies
Serves as the primary steering group for the statewide interoperability strategy. Its mission is to support the Statewide Interoperability Coordinator in efforts to improve emergency response communications across the state through enhanced data and voice communications interoperability. They often include representatives from various jurisdictions and disciplines, as well as subject matter experts.

Statewide Interoperability Executive Committees
Used interchangeably with Statewide Interoperability Governing Bodies.

Tactical Interoperable Communications Plan
A plan providing rapid provision of on-scene, incident-based mission-critical voice communications among all first responder agencies (e.g., emergency medical services, fire, and law enforcement), as appropriate for the incident, and in support of an incident command system as defined in the National Incident Management System.

Technical Assistance
Support to state, tribal, territorial, and local emergency responders and government officials through the development and delivery of training, tools, and onsite assistance to advance public safety interoperable communications capabilities.

Technology
Per the SAFECOM Interoperability Continuum, applies to a capability element that encompasses the systems and equipment that enable emergency responders to share information efficiently and securely during an emergency incident, and addresses the functionality, performance, interoperability, and continuity capabilities of those systems and equipment.

Telecommunications Service Priority
A DHS program that authorizes National Security/Emergency Preparedness organizations to receive priority treatment for vital voice and data circuits or other telecommunications services.
https://www.cisa.gov/cisa/telecommunications-service-priority-tsp

Threat and Hazard Identification and Risk Assessment
Required by several DHS grants, the Threat and Hazard Identification and Risk Assessment process helps communities understand threats and hazards and their varying impacts. The Threat and Hazard Identification and Risk Assessment process results in community-informed capability targets and resource requirements that are necessary to address anticipated and unanticipated risks.

Usage
Per the SAFECOM Interoperability Continuum, this applies to the frequency and familiarity with which emergency responders use interoperable emergency communications solutions.

Vulnerabilities
Weaknesses in a system, network, or asset that could enable an undesired outcome.

Wireless Priority Services
A DHS program that improves the connection capabilities for authorized National Security/Emergency Preparedness cell phone users, such as senior members of the presidential administration; local emergency managers; fire and police chiefs; technicians in wireline and wireless carriers; and managers of banks, nuclear facilities, and other vital national infrastructure.
https://www.cisa.gov/cisa/wireless-priority-service-wps

Whole Community

Per the National Preparedness Goal, the term whole community applies to the focus on enabling the participation in national preparedness activities of a wider range of players from the private and nonprofit sectors, including nongovernmental organizations and the general public, in conjunction with the participation of federal, state, tribal, territorial, and local governmental partners in order to foster better coordination and working relationships.

Appendix 6: Acronyms

CISA	Cybersecurity and Infrastructure Security Agency
DHS	Department of Homeland Security
FirstNet Authority	First Responder Network Authority
IPAWS	Integrated Public Alert and Warning System
IP	Internet Protocol
NECP	National Emergency Communications Plan

This page intentionally left blank.

Appendix 7: NECP Endorsement Letter

SAFECOM® NCSWIC®

TO:	Acting Secretary of the Department of Homeland Security
FROM:	Chief Gerald Reardon, SAFECOM Chair Joe Galvin, NCSWIC Chair
DATE:	April 24, 2019
SUBJECT:	**SAFECOM and National Council of Statewide Interoperability Coordinators (NCSWIC) Endorsement of the National Emergency Communications Plan (NECP)**

SAFECOM[1] and NCSWIC[2] have worked closely with Cybersecurity and Infrastructure Security Agency (CISA) staff and public safety communications stakeholders for over a year to update the NECP. In addition to offering our full support of the draft updates, we would like to thank CISA for the open and transparent process in which the updates were developed.

The importance of CISA's mission to coordinate emergency communications nationwide cannot be overstated. Our members serve their communities on the front lines protecting lives and property. The NECP serves as the backbone for this important coordination and nationwide progression to achieve operability, interoperability, and resiliency of emergency communications.

With increasingly-complex emergencies, rapidly-advancing technology, and tight budgets, the emergency communications community needs to be agile, cooperative, and organized. This is exactly the focus of the NECP update, which includes expanding and emphasizing cybersecurity planning and resources, establishing and leveraging shared services among organizations and jurisdictions, addressing adequate coordination and funding, and embracing new technologies and services, including FirstNet.

---

[1] **SAFECOM** was formed in 2001 to improve public safety interoperability, allowing emergency responders to communicate effectively before, during, and after emergencies and disasters. Comprised of X public safety associations representing all of the major disciplines, SAFECOM's mission is to improve designated emergency response providers' inter-jurisdictional and inter-disciplinary emergency communications interoperability through collaboration with emergency responders across Federal, State, local, tribal, and territorial governments, and international borders.

[2] **National Council of Statewide Interoperability Coordinators (NCSWIC)** promotes and coordinates activities designed to ensure the highest level of public safety communications across the nation. This direct approach improves interoperability and advances long-term emergency communications initiatives. Statewide Interoperability Coordinators (SWIC) strive to enhance the response capabilities of public safety responders by coordinating and collaborating with federal, state, local, and tribal public safety agencies and non-governmental organizations.

Both of our organizations look forward to working with DHS to implement the NECP to achieve its stated vision and goals. Thank you for your continued support as we work together to improve the emergency communications capabilities of our nation's first responders.

Sincerely,

Chief Gerald Reardon,
SAFECOM Chair

Joe Galvin
NCSWIC Chair