National Emergency Communications Plan

2019

Homeland Security

Table of Contents

Executive Summary

In 2008, the Department of Homeland Security (DHS) published the first National Emergency Communications Plan (NECP) to accelerate improvements for public safety communications nationwide. Title XVIII of the Homeland Security Act of 2002, as amended, directs the DHS Office of Emergency Communications—reestablished as the Cybersecurity and Infrastructure Security Agency (CISA)—to develop and periodically update the NECP in coordination with local, state, territorial, tribal, federal, and private sector stakeholders. The law also directs the NECP to set benchmarks for enhancing emergency communications capabilities and for CISA to measure progress toward achieving those milestones.

Given the range of changes public safety stakeholders face including rapid technological advancements, increasingly complex incidents, and constrained resources CISA has worked with stakeholders to update the NECP accordingly. The first update was released in 2014 and the 2019 version is the second update.

The NECP addresses many aspects of emergency communications, all impacted by the integration of technologies (e.g., land mobile radio; Next Generation 911; high-speed broadband; alerts, warnings, and notifications systems) and standard processes to support the interoperability of systems and services for voice, video, and information exchange among the responder and partner communities. Communities are preparing for the First Responder Network Authority's nationwide broadband communications platform to supplement existing systems and provide public safety users with dedicated spectrum, added broadband capabilities, and advanced technologies. However, network integration presents cybersecurity risks as a result of interconnected, Internet-based technologies. The NECP examines current challenges and opportunities for improving emergency communications capabilities in new goals for technology, infrastructure, and cybersecurity.

CISA collaborated with public safety community members nationwide to develop the third iteration of the NECP. 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, dispatch) and other entities that share information during emergencies, such as medical facilities, utilities, nongovernmental organizations, as well as the media and private citizens.

Given the diverse entities directly involved, supporting, or impacted by emergencies, the Emergency Communications Ecosystem concept expands to include the various functions and people that exchange information prior to, during, and after incidents. Individuals with roles in emergency communications are not limited to government agencies, traditional emergency responder disciplines, or jurisdictional boundaries. The Ecosystem is dynamic, depending on the incident or planned event. It is multi-directional—anyone can initiate emergency communications.

> "The Emergency Communications Ecosystem must support the whole 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

Over the next five years, CISA will focus on implementing the goals and objectives articulated in the NECP. These critical components for advancing emergency communications fall under three national priorities:

- Enhance effective governance across partners with a stake in emergency communications, embracing a shared responsibility of the whole community;
- Address interoperability challenges posed by rapid technology advancements and increased data sharing, ensuring critical information gets to the right people at the right time; and
- Build resilient and secure emergency communications systems to reduce cybersecurity threats and vulnerabilities.

To achieve these priorities, CISA centered the NECP around six goals that build on foundational concepts in the 2008 and 2014 plans, align to the SAFECOM Interoperability Continuum, and consider new risks and threats that need to be addressed today. The NECP goals are strategic in nature and aim to enhance emergency communications capabilities at all levels of government and in coordination with the private sector, nongovernmental organizations, and other key partners across the community. The six NECP goals are:

- **Goal 1 - Governance and Leadership:** Develop and maintain effective emergency communications governance and leadership across the 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 Ecosystem
- **Goal 3 – Training, Exercises, and Evaluation:** Develop and deliver training, exercise, and evaluation programs that 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 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

Within each goal, the NECP provides objectives for stakeholders to attain these goals, as well as defines success indicators that result from implementing the objectives. To implement the 2019 NECP, CISA will coordinate with public safety agencies and partners from across the Nation through partnerships such as SAFECOM, the Emergency Communications Preparedness Center, and the National Council of Statewide Interoperability Coordinators, among others. DHS and its partners will identify strategies to accomplish the NECP's goals and objectives, especially as they align with data collected and gaps reported in the Nationwide Communications Baseline Assessment. The NECP results will help DHS and public safety communications stakeholders target their resources to improve national capabilities.

The future of emergency communications is at a critical juncture. Through the NECP and the work of CISA and its partners, DHS is committed to supporting our Nation's emergency responders, including supporting organizations, decision makers, and citizens, as they strive to meet their missions and achieve the long-term vision of the NECP.

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 response to devastating natural disasters, active shooter incidents, terrorist threats, and routine events affecting our communities every day across America. 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 our whole community—every member contributes, including individuals, the private sector, non-profits, and all levels of government (e.g., local, state, territorial, tribal, federal).

Since the Department of Homeland Security's (DHS) establishment in 2003, one of its top priorities has been to improve communications capabilities among the public safety community. DHS 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 and the environment, stabilize communities, and meet basic human needs following an incident.

Emergency Communications

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

The Homeland Security Act of 2002 (6 United States Code § 572) as amended, provided renewed focus and vitality to this critical homeland security mission. The legislation established the DHS Office of Emergency Communications—which was reestablished as the Cybersecurity and Infrastructure Security Agency (CISA)—to lead development and implementation of a comprehensive approach to advancing national interoperable communications capabilities. To achieve this objective, the Act also 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." Appendix 1 details statutory requirements for the NECP.

National Priorities

Enhance effective governance across partners with a stake in emergency communications

Address interoperability challenges posed by rapid technology advancements and increased data sharing

Build resilient and secure emergency communications systems to reduce cyber threats and vulnerabilities

CISA collaborates closely with the public safety community to support and promote effective emergency communications through stakeholder-driven programs and services. Over the next five 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: first, to enhance effective governance across partners with a stake in emergency communications, embracing a shared

[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.

responsibility of the whole community, from traditional emergency responders and supporting entities to the citizens served; second, 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 third, to build resilient and secure emergency communications systems to reduce cybersecurity threats and vulnerabilities, as introduced through Internet Protocol (IP)-based technologies and services.

> The NECP establishes a strategy to enable the public safety community and citizens to communicate and share information securely across communications technologies in real-time

Purpose

As the Nation's strategic plan for emergency communications, the NECP establishes a vision ***to enable 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***. To achieve this vision, the NECP outlines nationwide goals and 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 is 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 tracks the many accomplishments since implementing the first NECP and understands the remaining hurdles to be cleared.

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

CISA conducted the SAFECOM Nationwide Survey and resulting 2018 Nationwide Communications Baseline Assessment, in which thousands of public safety agencies and organizations participated. Additionally, an extensive stakeholder engagement process was used to identify challenges facing emergency communications and propose solutions to address them. Representatives of major public safety organizations, government agencies, and key industry partners from the communications and information technology sectors provided input to the NECP. They recommended updating the NECP's vision, goals, and objectives to reflect current capability gaps and improvements needed to become a nationwide community that can exchange information securely at any time.

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 [EMS], dispatch) and other entities from the whole community that share information during events.

Progress

In the 2018 Nationwide Communications Baseline Assessment, respondents indicated an overall strengthening of emergency communications from 2011 to the present, with respondents from all disciplines and levels reporting improvement. For example, a range of 84 to 93 percent of state/territory respondents indicated either some or significant improvement in the strengthening of their communications operability, interoperability, or continuity. While these results show progress, findings also reflect 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 [IT] departments, private sector infrastructure owners).

Since the 2014 NECP, CISA continues to assist public safety to complete recommended activities 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.

Whole Community Partners

- Law Enforcement
- Fire
- Emergency Medical Services
- Dispatch
- Public Works and Services
- Public Health and Medical Facilities
- Transportation Agencies, Utilities, Critical Infrastructure Operators, and Commercial Service Providers
- Nongovernmental Organizations, International Partners, and Auxiliary Resources
- Media
- Private Citizens
- Elected and Appointed Officials, Local, State, Territorial, Tribal, and Federal Government Personnel

Organization of the NECP

The 2019 NECP supersedes the 2014 NECP and is effective immediately. The plan is organized as follows:

- **Emergency Communications Ecosystem**, which was first introduced in the 2014 NECP, has been refined and expanded to account for the role of citizens providing critical information.
- **NECP Strategic Goals**, as summarized in exhibit 1, establishes the strategy to meet national priorities and better position the whole community for the future of emergency communications.
- **Implementing the NECP** describes DHS 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.
- **Annex** expands descriptions of success indicators for the NECP goals and objectives.
- **Appendices** include Statutory Requirements Matrix, Key Authorities, Roles and Responsibilities, SAFECOM Interoperability Continuum, Source Documents, Glossary, and Acronyms.

Exhibit 1: NECP Strategy

Emergency Communications Ecosystem

Since the first NECP publication 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 and integrate new technologies, and mitigate growing cyber threats. These efforts are not constrained within the limits of traditional emergency response of law enforcement, fire, EMS, and dispatch. 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—a concept referred to as the Emergency Communications Ecosystem.

> The Emergency Communications Ecosystem is comprised of the various functions and people that exchange information prior to, during, and after incidents

The public safety community continues to prioritize maintaining land mobile radio (LMR) and data exchange systems and improving operability, interoperability, and resiliency. Emergency responders are also embracing emerging technologies and integrating them with existing systems. With the First Responder Network Authority's (FirstNet) 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. 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 other entities that also exchange information during emergencies, such as medical facilities, critical infrastructure operators, and citizens. While these individuals are not typically trained responders, they can share valuable information during response and recovery efforts. Social media use is increasing. Responders need to develop best practices for engaging with the public, and analyzing 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.

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 (NIMS) 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—Prevention, Protection, Mitigation, and Recovery.

Incorporating the National Response Framework and NIMS 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. The Ecosystem is dynamic, not everyone is needed every day depending on the incident or planned event. It is also multi-directional, as anyone can initiate emergency communications, including supporting entities or private citizens.

> "The NECP is a forward-thinking document—one that anticipates risks and threats related to technology rolling out down the road; it is about the evolution of the Emergency Communications Ecosystem."
>
> Vincent DeLaurentis, Deputy Assistant Director for Emergency Communications, CISA

As a potential scenario of the Emergency Communications Ecosystem in action, consider the following:

The neighbors were posting social media messages complaining about the strange odors they were smelling in addition to abnormal numbers of people and vehicles at all hours around the neighborhood. These messages posted to city/county government, public works, political leaders, and law enforcement culminated in initial investigation by local law enforcement, including monitoring social media traffic. Bolstered by additional information from Text-to-911 messages received by the Public Safety Answering Point (PSAP), 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 order of toxic chemicals overwhelmed them, and as they backed out, they spotted some booby traps within steps of their entryway. Body cameras on the entry team members recorded the activities, the observed illicit lab and chemical components stockpiled in the residence, and provided initial details of the booby trap devices. The local fire department, paramedics, and the state police bomb squad were requested. The local emergency manager and the PSAP 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 PSAP used their public alert system to make calls and send short text messages to inform neighbors' evacuation orders and shelter resources. The public information officer alerted the media and the public using social media and broadcast news resources about the 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 the same encrypted radio channel to coordinate their efforts. A command post and unified command were established, with personnel using the Nationwide Public Safety Broadband Network to support administrative 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.

Understanding the Ecosystem, exhibit 2, provides agencies with a full picture of emergency communications functions necessary to achieve reliable, secure, and interoperable emergency communications, which include:

reporting and requests for assistance; incident coordination and response; alerts, warnings, and notifications; and public interaction. These primary functions, the timeframes when they occur, their purpose, and examples of each are listed below.

Communications Functions	Timeframe	Purpose	Examples
Reporting & Requesting Assistance	During and after incidents	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	Prior to, during, and after incidents	Direct voice and data communications between public safety responders 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	Prior to, during, and after incidents with an ongoing immediate threat	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
Public Interaction	Anytime	Publics' sharing of information through various public or commercial networks supporting Internet, social media, and telephony communications	Telephone calls, social media, such as Facebook, Twitter, web services and applications

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 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 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 day-to-day efforts or out-of-the-ordinary, large-scale events. 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 (i.e., law enforcement, fire, EMS, and dispatch). With the adoption and integration of new technologies, governance is an initial step toward preparing first responders to manage increased information and data exchange across organizations and the risks they bring. 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 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, such as Statewide Interoperability Governing Bodies (SIGBs), Statewide Interoperability Executive Committees (SIECs), 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. 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.

> 'SWICs 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 SWIC, NCSWIC Vice Chair

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. For instance, the Statewide Interoperability Coordinator (SWIC) plans and executes the statewide interoperability program, guided by stakeholder-driven initiatives in the NECP and the Statewide Communication

Interoperability Plan (SCIP) and implemented by Tactical Interoperability Communications Plans (TICPs).

As such, SWICs 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. Despite the benefits of having a full-time SWIC, exhibit 3 demonstrates a decline in overall SWICs between 2010 and 2017. Federal departments and agencies and tribes also benefit from having a similar coordination point or governance mechanism parallel to the SWIC to implement interoperability policies, decisions, and processes currently 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 SIGBs*
- ✓ *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 SWIC in each state or territory, such as the development of legislative language and mandates*
- ✓ *State and territory governance bodies prioritize communications needs and coordinate with the SWIC 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 Your SWIC

Since 2010, full-time SWIC positions have declined 70%, from 44 to 12. In the remaining states, the SWIC 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 heavily rely on SWICs to translate technical issues into policy and coordinate cost-effective solutions for maintaining legacy systems and integrating new technologies.

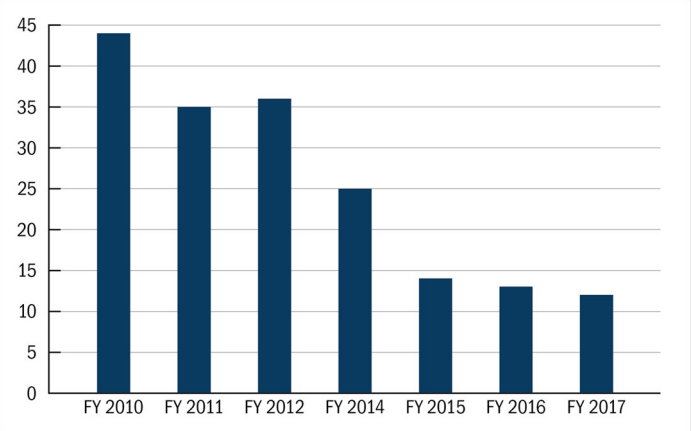


Exhibit 3. Decline in full-time SWICs from 2010-2017

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

Supporting Your State 911 Administrator

The State 911 Administrator manages 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, with a clearly defined 911 program coordination role, 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, EMS, nongovernmental organizations (NGOs), public works, utilities, forestry services, military, private sector, and the American Red Cross, etc. 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.

Tribal Resources for Coordination

Developing collaborative and trusted relationships between 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 from surrounding tribal nations on local, regional, and state governance, as requested by and coordinated with tribes.

As the Nation experiences unprecedented changes in system connectivity, the types of technologies used, and the flow and potential exposure of data, IT officers, such as the Chief Information Officer, bring technical expertise and increases public safety community end-user-coordination. Their participation on subcommittees related to new technologies, threats, and issues provides subject matter expertise when coordinating the integration of IP-based and advanced technologies. Formal participation of elected officials and decision makers allows those making fiscal and policy decisions to better understand emergency communications priorities, empowering them to take informed action. Formal collaboration also 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 partners (i.e., jurisdictions, tribes, sectors, organizations) in formal governance structures, when developing strategic and operational plans and policies, and 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*

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

Building resilient emergency communications is dependent on our capacity to adapt when facing sudden disruption or ongoing, slow-moving change, such as the adoption of a new technology. 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 (e.g., voice, text, video, data) and smart spectrum optimization, or mitigating their associated risks (e.g., cyber-attacks, interoperability), such as amendments to policy, regulation, and funding for more effective cybersecurity.

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 and the need to identify alternative resources (economic). Adaptive governance models may also consider a phased approach to strategic planning, 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

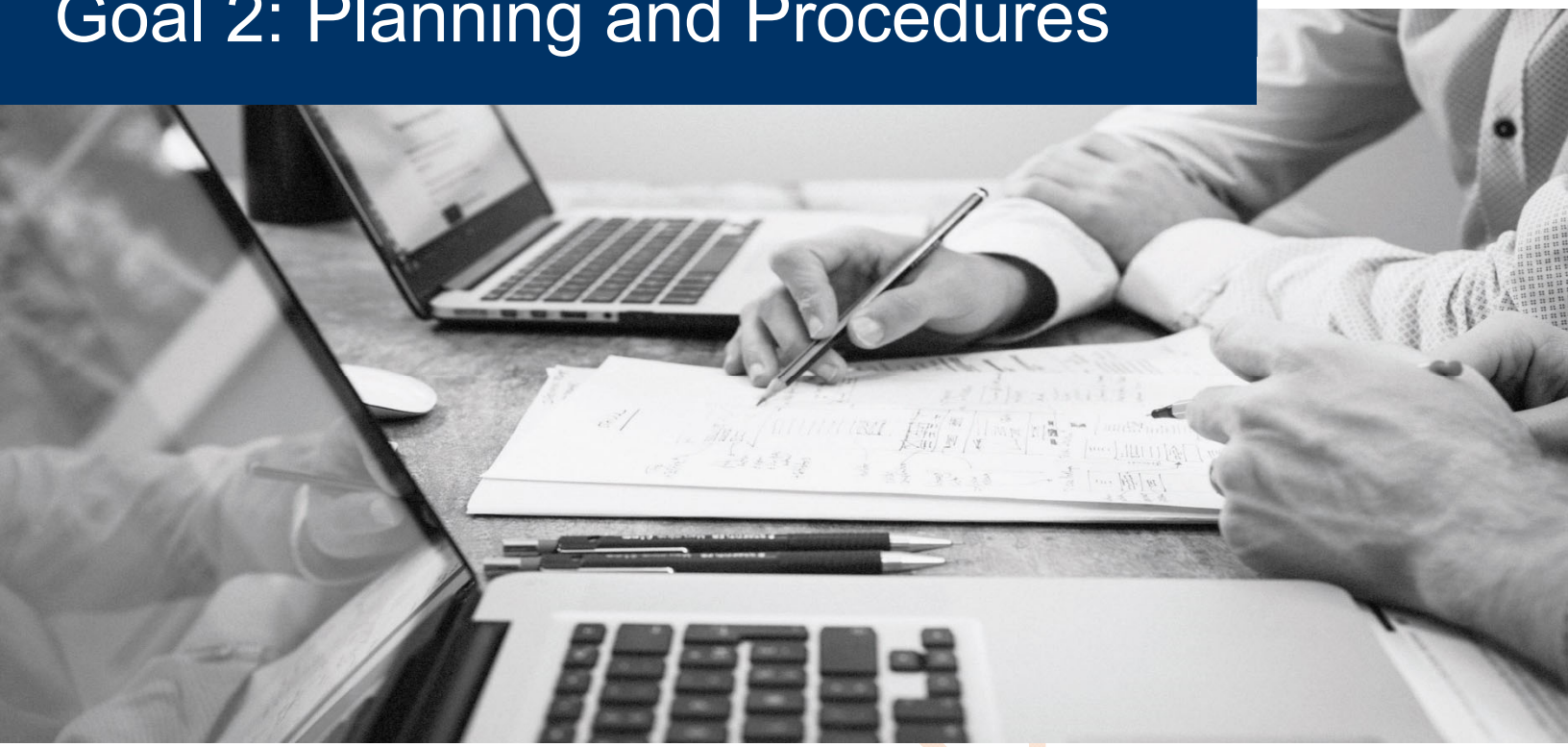
- ✓ *Governance bodies undertake technology integration and migration initiatives (e.g., broadband, 911, alerts and warnings, information management, network infrastructure, cybersecurity) to guide implementation by public safety*
- ✓ *Governance bodies identify and address legislative and regulatory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

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

Adapting Foundational Governance Practices: 2018 SAFECOM and NCSWIC Governance Guides

In 2018, SAFECOM and the NCSWIC 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 best practices for resource coordination, funding and sustaining interoperability, partnership formation, and 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 Ecosystem

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

Given the rapidly evolving emergency communications and IT 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 personnel and training needs 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 interoperability issues. Effective strategic plans consider multi-jurisdictional needs, standardization of technology interfaces in their own 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 new partners, such as private and health sectors; legal and policy aspects of information and data sharing; funding support for integration and interface; security concerns and solutions; and preparations for forward compatibility of evolving technologies.

The SCIP is the primary emergency communications strategy for each state or territory, defining critical emergency communications capabilities and needs. States and territories work with SWICs to align investments with SCIPs and individual implementation plans to improve communications. Since many federal emergency communications grants require recipients to align their projects to the SCIP, local, state, territorial, and tribal public safety agencies benefit from contributing to the development or revision of SCIP content as it pertains to priorities across communities. For federal departments and agencies, the ECPC works with personnel 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., SCIPs, Regional Interoperability Communications Plans, Next Generation 911 [NG911] Plans, Cybersecurity Plans) to measure progress against NECP objectives and any additional state or territory objectives, and update plans annually*

- ✓ *Federal departments or agencies develop emergency communications strategic plans in coordination with the ECPC*

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

Public safety organizations rely on complex, often expensive, systems to carry out their missions. According to findings from 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, and 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 evolution. Consideration of short- and long-term evolution enables an organization to determine its 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, including allowable costs and applicable standards. 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 NCSWIC Emergency Communications System Lifecycle Planning Guide's recommendations, checklists, and suggested timelines. Public safety increasingly understands the need to diversify funding mechanisms and resources in their efforts to prioritize system sustainment and upgrade, as detailed in the 2018 SAFECOM and NCSWIC Funding Mechanisms for Public Safety Communications Systems, which lists real-world examples for other agencies to consider. The following are indicators of success for this objective.

Success Indicators

- ✓ *Federal funding authorities develop federal 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 our emergency communications systems (e.g., Internet of Things [IoT], next generation technologies, data interoperability, social media, encryption) brings a wealth of new capabilities, as well as associated risks (e.g., system failure, cyber-attacks, data breaches). The DHS Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR) are helpful when conducting state-level, emergency communications capability evaluations. Communities participate in these

interconnected processes to evaluate preparedness, including capabilities for emergency communications. Local and state decision makers and SWICs 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 personnel who run them also 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, as shown in exhibit 4. Incident Response Teams (IRTs), incident response plans, recovery or resiliency plans, and continuity of operations (COOP) plans are useful in cybersecurity incident response. IT administrators may consider establishing a Computer Security Incident Response Team (CSIRT) or reach an agreement with the U.S. Computer Emergency Readiness Team (US-CERT), run by DHS National Cybersecurity and Communications Integration Center (NCCIC), to assist in cybersecurity planning. Additionally, coordinating response and recovery efforts with the SWIC and other IT administrators can increase cybersecurity posture. The following are indicators of success for this objective.

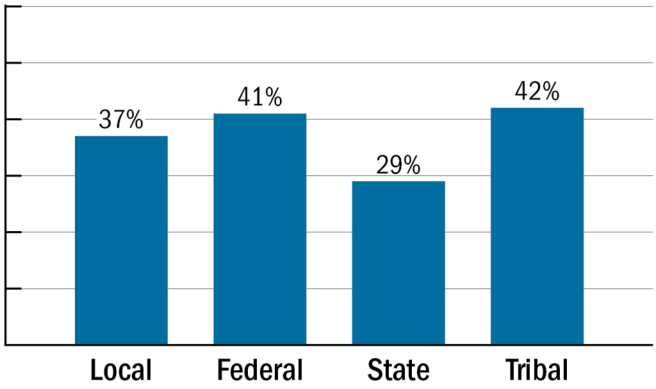
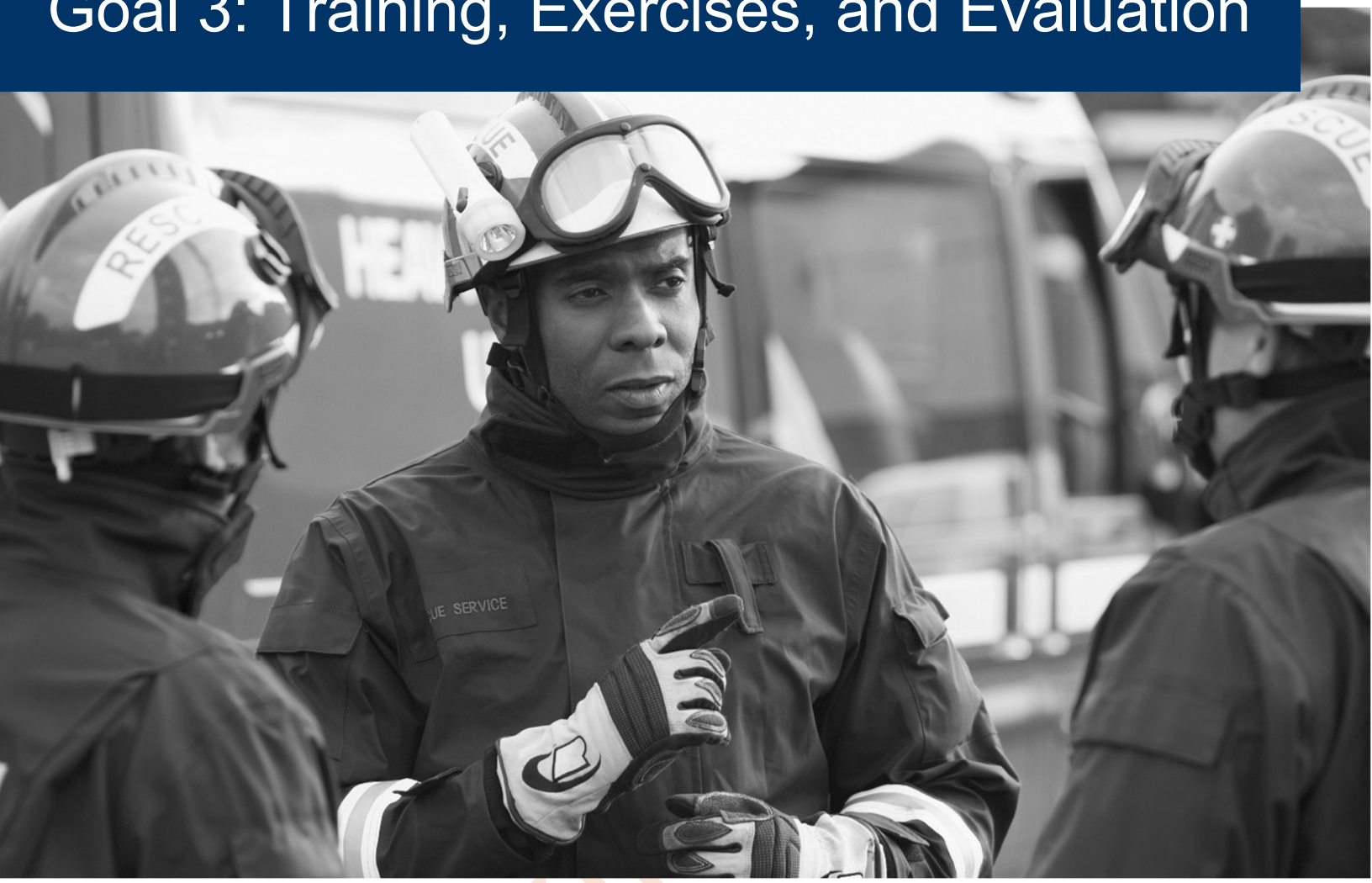


Exhibit 4. Percentage of public safety organizations whose strategic planning process does not ensure continuity in out-of-the-ordinary situations

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., THIRA, SPR)*
- ✓ *Public safety organizations incorporate risk management strategies into plans for continuity and recovery of critical communications*
- ✓ *Public safety organizations that use IT 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 target gaps in all available emergency communications technologies

Objective 3.1: Update and implement 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, data, and video information place on personnel

Objective 3.3: Ensure training addresses information sharing (i.e., voice, video, 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 NIMS/Incident Command System (ICS)-capable communications support personnel.

Objective 3.1. Update and ensure the availability of training and exercises 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 exhibit 5, 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 exercise. 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 (SOPs), partners, and technologies as they occur.

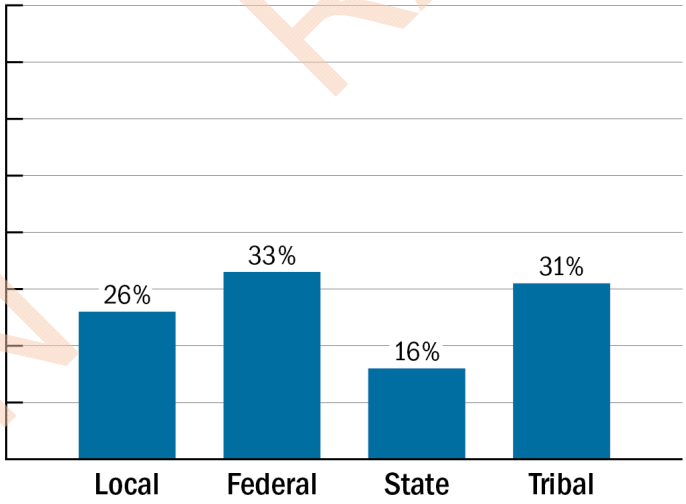


Exhibit 5. Percentage of public safety organizations that do not participate in exercises

Assessment of communications during exercises and real-world events and incidents allows public safety organizations to 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 (AARs). Outcomes-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 with solutions to strengthen communications coordination.

The Homeland Security Exercise and Evaluation Program (HSEEP) is the national standard for developing exercises with objectives supported by exercise evaluation guidelines. Public safety 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 Now Available

DHS has posted a series of technical how-to training videos covering many aspects of Government Emergency Telecommunications Service (GETS), Wireless Priority Service (WPS), and Telecommunications Service Priority (TSP), as well as a half-hour video webinar on all three programs. The how-to videos run approximately three to four minutes each and cover:

- How to Enroll in GETS, WPS, and TSP
- How to Make a GETS Call
- How to Make a WPS Call
- What to Do When the GETS Access Number Doesn't Work
- Programming GETS/WPS into your Phone Contacts List
- How to Request Provisioning or Restoration Once Enrolled in TSP

The videos and webinar are available at www.dhs.gov/pts-videos.

Evaluations are only effective if training and exercise programs are improved because of the 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, and continuity of communications*
- ✓ *Public safety organizations offer training classes and exercises across multiple agencies and jurisdictions 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 system and personnel (including emerging technology and system failure) and utilize third-party evaluators with communications expertise*
- ✓ *Public safety organizations integrate private sector, NGOs, and public sector communications stakeholders into training and exercises*
- ✓ *The ECPC 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, data, and video information place on personnel

Training resources must keep pace with the integration of new communications technologies and services added to public safety professionals' available capabilities. More technologies and applications result in more data to process, more SOPs 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 from previous lessons, adding new objectives along the way. Progressive training and exercises not only build upon each other, but also increase repetition of use to develop "muscle memory," leading to the likelihood of available technologies used appropriately and effectively during incidents and planned events.

One downside to repetition is impacts to personnel from recurring exposure to incident scene images, which can increase the risk of post-traumatic stress. 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 even 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. 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 implementing NG911 utilize training and resources to address the impact of incident images/videos on dispatchers*

Objective 3.3. Ensure training addresses information sharing (i.e., voice, video, 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 (COMLs) and Communications Technicians (COMTs) have been trained, agency leadership often do not know or take advantage of this capability during actual responses. Accessing these resources is difficult when not every state has a program with policies and procedures to track, maintain, and utilize NIMS/ICS-capable communications support resources. The NECP promotes progress for Emergency Support Function #2 (ESF-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 (ITSL) to address increased demand for IT devices and networks during an incident or planned event. The ITSL Course ensures that communications support resources are equipped with adequate skills to operate and troubleshoot IT 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 local, state, territory, tribal, and federal 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 NCSWIC 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 NIMS and ICS, Communications Unit personnel plan and manage the technical and operational aspects of the communications function during an incident or event. To obtain Communications Unit, COML, or COMT status, trainees must complete a Position Task Book (PTB) documenting their ability to perform the functions required of a Communications Unit position. The NCSWIC Planning, Training, and Exercise Committee, in conjunction with the SAFECOM Communications Section Task Force, developed a PTB Sign-Off Process Template to assist SWICs, SWIC designees, state governance bodies, and regional governance bodies in developing a system for Communications Unit personnel PTB 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 and active use of the NIMS doctrine

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 is critical to ensure both responder safety and the timely provision of public safety services. Being familiar with the operation and use of available capabilities prior to a response minimizes communications challenges during an incident. Similarly, the advantages realized from 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 AARs reflect improvements in coordination through the use of communications technologies, challenges remain due to continuous technological advancements.

> Effective coordination and efficient usage of all available communications capabilities is critical to ensure both responder safety and the timely provision of public safety services

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 commercial and non-traditional communications systems providers.

Objective 4.1. Confirm the implementation and active use of the NIMS doctrine

Public safety organizations use NIMS and ICS 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 NIMS and ICS 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 (IC) or Incident Management Team (IMT) remain informed about the status of all available operable and interoperable communications capabilities through sharing appropriate ICS form(s).

Public safety organizations of all disciplines are experiencing increased information sharing from various reporting sources when larger complements of communications resources are deployed during initial responses to incidents. These heightened responses require pre-planning between public safety organizations, IC and IMT personnel, and communications systems providers. This coordination highlights the value of including providers and helps responders be more aware and comfortable with expected timelines for their inclusion, resulting in 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 NIMS and ICS and share appropriate forms (e.g., ICS 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 IC and IMT 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 increase 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. Providers may be internal, external, or a combination of both, and their expertise, knowledge, information, 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.

To coordinate various communications tools, knowing the availability and current state of all operable and interoperable assets is critical. At a minimum, public safety organizations need to share current communications systems information with contiguous public safety agencies and other organizations which provide or receive mutual aid, share infrastructure, or participate in planned events. Sharing active, available features, functionality, and capabilities of communications capabilities 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, SOPs, tactical response directives, and/or TICPs 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, utilities) in incidents and planned events*

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

As of 2018, a significant percentage of public safety agencies, nearly 25 percent, lacked SOPs on emergency communications. However, the fast-paced evolution of communications capabilities highlights a crucial need to update—and develop, if they do not exist—SOPs and operational plans to address entities, individuals, or organizations that provide or use communications during emergencies (e.g., utilities, transportation sector, commercial carriers). Coupled with effective planning, training, and exercises, SOPs transform policy and best practices into real-world understanding of operational plans, which detail how to establish and maintain communications during an incident or disaster. Analyzing AARs following events can assist with resolving gaps or missing information through the development or revision of SOPs.

SAFECOM SOPs Resources

Visit the SAFECOM website to learn more about how to develop policies for coordinating interoperability during incident response, including tips for communities developing SOPs, 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 an end-user's ability 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, established by set minimum standards, in the use of communications capabilities drive appropriate recommendations for modifications and expansion of user instructional documentation, informal and formal trainings, drills, exercises, and SOPs. The following are indicators of success for this objective.

Success Indicators

- ✓ *Public safety organizations develop and regularly update NIMS-aligned SOPs to facilitate the integration, deployment, and use of communications assets*
- ✓ *Public safety organizations have recommended guidelines developed on 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 SOPs*
- ✓ *Public safety organizations periodically review the priority service programs (e.g., TSP, GETS, WPS) to which they subscribe and ensure they have SOPs governing the programs' use, execution, and testing*
- ✓ *Public safety organizations periodically test 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, LMR systems may need to be augmented by air 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 damage or congestion 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 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 from 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*
- ✓ *PSAPs, Public Safety Communications Centers (PSCCs), and Emergency Operations Centers (EOCs) address systems and staffing to support communications COOP planning*
- ✓ *SAFECOM and the NCSWIC 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 are collaborating on a single, actively shared federal LMR 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 can be expensive and disrupt mission critical operations and communications. Yet, emerging technologies, such as wireless data networks and IP-based 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 communications 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 the rollout of FirstNet and greater 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 (P25) radio systems and NG911 are being deployed. The public safety community continues to develop strategies and technology roadmaps for implementing standards-based, open-source, 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 NCSWIC identify public safety technology and infrastructure capability gaps*
- ✓ *The ECPC coordinates federal research, development, testing, and evaluation priorities and processes*
- ✓ *The ECPC cultivates sustained engagement (e.g., cooperative agreements) between federal research, development, testing, and evaluation programs, such as DHS Science and Technology Directorate and the National Institute of Standards and Technology (NIST) Public Safety Communications Research Division (PSCR), and public safety organizations focused on resiliency, interoperability, and other challenges*
- ✓ *The ECPC 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

FirstNet Technology and Infrastructure Activities

- Establish a dedicated (physically-separate) Public Safety Long-Term Evolution (LTE) 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 deployables plus access to hundreds of existing LTE deployables
- Accelerate delivery of mission critical LTE services, such as mission

Public safety 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—improving operability, interoperability, and security. Programs that facilitate technology adoption are necessary to communicate benefits and minimize risk. Not every new or enhanced technology will be appropriate for each unique public safety organization's mission, nor can a new or enhanced technology be adopted without consideration of impacts to governance, SOPs, use, training, and exercises. The following are indicators of success for this objective.

Success Indicators

✓ *SAFECOM and the NCSWIC communicate emerging technology impacts to public safety, such as those associated with identity management, multimedia, 5G, IoT, social media, network virtualization, spectrum optimization, artificial intelligence, machine intelligence, geographic information systems, and positioning, navigation, and timing systems*

✓ *SAFECOM and the NCSWIC guide standards-based LMR evolution*

National 911 Program NG911 Technology and Infrastructure Activities

- Convert all addressing to geographic information system
- Establish dedicated Emergency Services Internet (ESInet) and NG911 Core Services
- Install NG911-capable and standard-compliant 911 Customer Premises Equipment (CPE) and Computer-Aided-Dispatch (CAD)
- 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, CAD, and FirstNet
- Develop and rapidly adopt technical models to manage the receipt, processing, and sharing of multimedia

- ✓ *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 NG911*

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 since 2014, shaping the way information is communicated and shared. Emerging capabilities expand with whom and how agencies can share information before, during, and throughout 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. In the 2018 Nationwide Communications Baseline Assessment, on average, less than half of public safety organizations use or test interoperability solutions for data, as shown in exhibit six. One challenge for effective information exchange includes the increasing types of data being exchanged, such as video, geographic information system (GIS) data, evacuee/patient tracking data, accident/crash (telematics) data, biometric data, CAD data, Automatic Vehicle Location (AVL) data, Common Operation Picture data, and more.

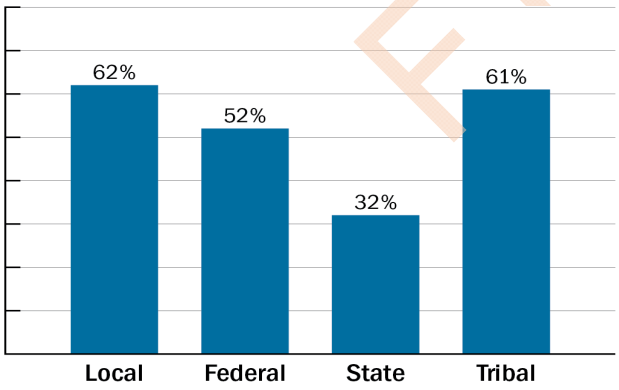


Exhibit 6. Percentage of public safety organizations that never use or test interoperability solutions for data

Another challenge is the volume of data requiring storage, exchange, maintenance, and analysis. 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, IoT, 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 NCSWIC publish best practices and updated guidance on SOPs to assist the public safety community in meeting 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

The time for instituting a "security first" perspective for emergency communications is now. To prepare for cyber-attacks, the public safety community must continually identify risks and address evolving security requirements in coordination with partners in their Emergency Communications Ecosystem. Cybersecurity is a shared mission across all levels of government, the private sector, NGOs, and even 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 assist organizations in managing their cybersecurity risk. For example, organizations can request self-assessments or onsite assessments from DHS's Cyber Resilience Review program to uncover gaps and areas for improvement. In addition, DHS established the National Risk Management Center to create a cross-cutting risk management approach between the private sector and government to improve the defense of the Nation's critical infrastructure.

As cyber threats grow in complexity and sophistication, attacks could 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 to identify and prioritize risks, protect resources, detect threats, and establish response and recovery processes. Despite every effort, cyber threat events will occur. Exhibit 7 shows the significant percentages of public safety organizations affected by cybersecurity, according to results from the 2018 Nationwide Communications Baseline Assessment. Being prepared to execute response processes and procedures, prevent expansion of the event, mitigate its effects, and eradicate the incident is necessary. Incident response plans, recovery or resiliency plans, and COOP plans are useful in 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.

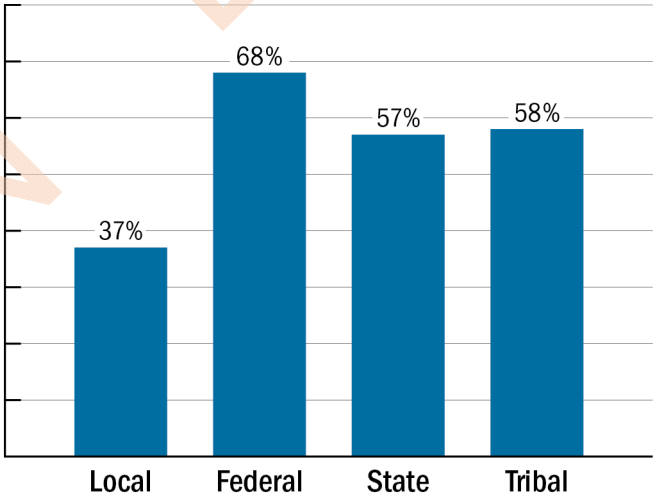


Exhibit 7. Percentage of public safety organizations whose communications have been impacted by cybersecurity breaches at some point in the last 5 years

Success Indicators

- ✓ *Public safety organizations, at a minimum, implement the Cybersecurity Framework*
- ✓ *Public safety organizations use the Critical Infrastructure Cyber Community Voluntary Program (C³ Voluntary Program)*

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 organization's cybersecurity risk. They must also consider the impacts of their cybersecurity risk management on interoperability with the broader community. 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

Look up guidance on encryption and key management, such as the Best Practices for Public Safety Interoperable Communications.

SAFECOM and the NCSWIC continue to produce guidance educating the community on known mid- and long-term threats and their mitigations. Voice and data encryption is increasingly in use throughout the public safety community as another means to mitigating threats, but not without challenges. For example, encryption can add a significant level of complexity and should be considered only when operational requirements of the incident outweigh additional complications. Another important aspect of cybersecurity is a comprehensive review of the standardized protocols and proprietary mechanisms connecting devices to and through the Internet. NIST should review protocol standards, as well as provide cybersecurity testing and certification activities, for the public safety community. The following are indicators of success for this objective.

Success Indicators

- ✓ *SAFECOM and the NCSWIC share planning and mitigation guidance regarding known threats and vulnerabilities*
- ✓ *Public safety organizations implement interoperable encryption, as needed*
- ✓ *SAFECOM and the NCSWIC refine the NG911 Emergency Communications Center (EC3) concept*
- ✓ *NIST evaluates 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 for the significant costs of these activities. The 2018 Nationwide Communications Baseline Assessment revealed the significant percentage of public safety organizations that lack funding to address their cybersecurity needs, as shown in exhibit 8.

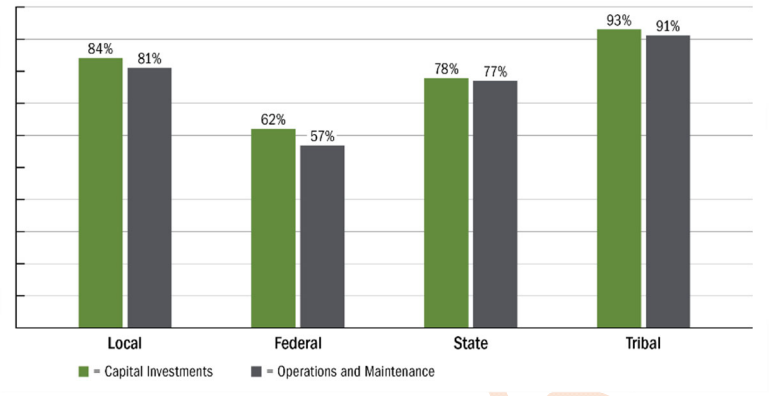


Exhibit 8. Percentage of public safety organizations that have no funding or insufficient funding to meet cybersecurity needs

Cybersecurity is a continual process of enhancing defense. Some organizations will have less capacity than others to apply for and manage grants. Therefore, NIST should work to develop a plan for setting, testing, and maintaining cyber minimum standards to assist cybersecurity-eligible grant programs in distributing necessary funding to public safety. To promote the importance of cybersecurity to operability and interoperability, cybersecurity 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

- ✓ *NIST establishes public safety-specific, standards-based cyber hygiene minimums for public safety*
- ✓ *SAFECOM updates the Interoperability Continuum to account for cybersecurity*
- ✓ *SAFECOM and the NCSWIC 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*
- ✓ *National Risk Management Center provides a cost study of public safety cybersecurity risk management and evaluates the need for additional grant programs*
- ✓ *NIST provides incentives for 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 office will use a two-step approach to 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 and campaign to promote the NECP. Both steps will be coordinated in partnership with stakeholders from the public safety community.

Although DHS leads the development and management of the NECP, the implementation is a shared responsibility among the Department and the plan's stakeholders. This reflects the nature of the public safety community, which spans disciplines, jurisdictions, and levels of government, and also involves the public and private sectors. As such, the action plan will identify supporting actions that CISA programs, services, or offerings can update or modify, develop, and enact to implement the NECP. It will further coordinate with local, state, territorial, tribal, and federal 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 towards its desired end-state as described in the NECP vision. CISA will enlist its Regional Coordinator personnel and "champions" from the local, state, territorial, tribal, and federal 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—consistent evaluation of how well communications function during response operations is a major challenge that requires cooperation at all levels of government.

CISA will assess progress in achieving the 2019 NECP goals and objectives using 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 towards the individual objectives
- Assess the collective progress of objectives to indicate progress towards 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 2019 NECP
- Conduct a periodic collective assessment of 2019 NECP goals and the 2023 Nationwide Communications Baseline Assessment to track progress towards the plan's overall implementation

The 2019 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 via the next Nationwide Communications Baseline Assessment. CISA conducts the assessment every five 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 gauge implementation of the NECP, as well as inform the development and update of the next iteration.

Reporting

In accordance with 6 U.S.C. § 573, 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 2019 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 build on previous successes and pursue opportunities for improvement. The 2019 NECP emphasizes the close collaboration by 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 is more than a plan; it is recognition of a complex Emergency Communications Ecosystem, which must respond seamlessly to any incident—natural or man-made—and remain secure in a world of ever-evolving threats to our communities."
> Ron Hewitt, Assistant Director for Emergency Communications, CISA

To that end, the NECP sets forth six strategic goals to advance the capabilities needed for operational success in an increasingly 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 our Nation's emergency responders and supporting entities can fulfill their mission needs in a seamless and fully interoperable, next generation Emergency Communications Ecosystem.

Annex I: Success Indicator Descriptions

Goal 1 - Governance and leadership: Develop and maintain effective emergency communications governance and leadership across the 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 SIGBs

Formal governance structures, such as Statewide Interoperability Governing Bodies (SIGBs), Statewide Interoperability Executive Committees (SIECs), 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 their 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 bylaws document 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, defines administrative duties, and outlines the organizational structure and voting processes for decision-making in the group. The charter's value increases when buy-in is sought and granted by members of the governance body, encouraging commitment to the group's purpose and decision-making strategies, and language remains flexible for adapting its membership, structures, and processes to the evolution of emergency communications.

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

The SWIC'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 (SCIP). As such, SWICs 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, SWICs are responsible for the implementation of the SCIP, which establishes a vision for interoperability across the state. SWICs also execute the grant application process, coordinating decisions on communications investments funded through federal grants to ensure projects align with the SCIPs and are compatible with surrounding systems.

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

In accordance with the FY 2018 SAFECOM Guidance on Emergency Communications Grants, states and territories are encouraged to coordinate the SWIC and state-level planners (e.g., broadband and 911 planners, utilities commissions), as well as the State Administrative Agency (SAA), to ensure projects and investments align with statewide plans and technical compliance requirements. The SAA, or an equivalent role, administers all homeland security and emergency communications grant funding for the state and 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 SAA, in coordination with the SWIC, is also a good resource for assisting with the State Preparedness Report, regional and state strategic plans, and project alignment at the local level with the state's long-term vision for interoperability. For instance, the SWIC may escalate policy and grant recommendations to the SAA 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 scattered 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 partners (i.e., jurisdictions, tribes, sectors, 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 involved in decision-making processes to prevent them. 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 on 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, local, and regional 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 (MOUs/MOAs) to define how information, resources, and infrastructure may be shared. Involvement of tribal points of contact is necessary since 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 (IT) officers, such as the Chief Information Officer (CIO), to participate in emergency communications governance bodies increases IT 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 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 provides elected officials and other decision makers 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. This approach emphasizes the need for direct discourse between public safety organizations and those forming policy to determine a tangible path toward interoperability resilience.

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

Success Indicators

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

As communications technologies converge, experts who oversee land mobile radio (LMR), broadband/long-term evolution (LTE), 911/Next Generation 911 (NG911), alerts and warnings, IT 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 avoid duplication of efforts and ensure consistent and coordinated deployment of technologies across existing systems. This approach ensures individual system plans (e.g., statewide 911 plan, statewide cybersecurity strategy) align with the SCIP and overall strategies for achieving interoperability.

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

Implementation of new and emerging technology requires awareness and compliance with certain legislative and regulatory constraints surrounding public safety. For example, the First Responder Network Authority (FirstNet) is 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 legislature that either limits or enables implementation of the network and its technology. Periodic reviews of federal, state and local regulations affecting public safety and emergency communications technology inform governing bodies and public safety organizations of funding opportunities, as well as any possible restrictions in securing emerging technology.

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

MOUs, MOAs, or MAAs minimize risks for the communities they serve by supplementing informal relationships between agencies, which are often limited in scope and duration. However, few public safety organizations work with their 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. An MOU or MOA may also define party responsibilities for a shared system, provide its scope and authority, outline compliance issues, and even streamline processes for grant fund application or award. 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 (ECPC) 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 the integration of new capabilities into their operations. The ECPC plays a valuable role assisting agencies to navigate challenges and realize opportunities associated with transitions to new capabilities. Public safety organizations follow the ECPC to learn more 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 Ecosystem

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

Success Indicators

Public safety organizations use strategic implementation plans (e.g., SCIPs, Regional Interoperability Communications Plans, NG911 Plans, Cybersecurity Plans) to measure progress against NECP objectives and any additional state or territory objectives, and update plans annually

The SCIP is the primary strategic implementation plan for each state and territory, defining critical emergency communications capabilities and needs. The SCIP outlines recommendations from the public safety community 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 SWIC to ensure investments support, and do not contradict, statewide plans, and align with the NECP goals and objectives. Since many federal emergency communications grants require recipients to align their projects to the SCIP and SCIP Annual Snapshot, public safety agencies benefit by contributing to the development or revision of SCIP content as it pertains to priorities across communities. An overarching statewide/territory-wide emergency communications plan helps states/territories align the efforts or its stakeholders 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 ECPC

Given the rapidly evolving emergency communications and IT environment, it is critical federal departments and agencies plan for new investments, maintain and modernize legacy systems, and identify personnel and training needs 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 look different from agency to agency, the ECPC 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 federal 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, 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 back-up systems

Successful lifecycle plans take each phase of SAFECOM and NCSWIC's lifecycle planning model into account and include input from project planners, decision-makers, and other stakeholder as necessary. The plan also consolidates 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, 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 structure and build major sections of their plan.

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. As detailed in the 2018 SAFECOM and NCSWIC Funding Mechanisms for Public Safety Communications Systems, examples of alternatives to grant funds include bonds, public-private partnerships, user fees, 911 surcharges, traffic ticket and vehicle surcharges, leasing equipment and infrastructure from public and private entities, grants, and other unique streams. The Emergency Communications System Lifecycle Planning Guide also describes the lifecycle planning model and provides strategies for funding system purchase, maintenance, and upgrade.

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. THIRA, SPR)

The DHS Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR) are helpful when conducting state-level, emergency communications capability evaluations. All types of communities participate in these interconnected processes to evaluate community preparedness. Local and state decisions makers and SWICs 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 personnel who run them help to prevent catastrophic loss of critical communications to end-users during emergencies or disasters. Despite its importance, however, 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 minimum communications requirements to perform essential functions and alternate equipment and systems, staff and their responsibilities, and facilities or base locations. From a purely network resiliency perspective, three key elements to consider when planning include route diversity, or routing between two points over one geographic or physical path with no common points; redundancy, when additional or duplicate communications assets share the load or provide back-up to the primary asset; and protective and restorative measures to decrease the likelihood a threat will affect a network and the latter which enables rapid reestablishment of services if disabled or destroyed, such as through DHS's Telecommunications Service Priority (TSP). Additionally, COOP 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 (i.e., TSP, Government Emergency Telecommunications Service, Wireless Priority Service).

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

Incident Response Teams (IRTs), incident response plans, recovery or resiliency plans, and COOP plans are useful in cybersecurity incident response. IT administrators may consider establishing a Computer Security Incident Response Team (CSIRT) or reach an agreement with the U.S. Computer Emergency Readiness Team (US-CERT) US-CERT, run by DHS National Cybersecurity and Communications Integration Center (NCCIC), to assist in cybersecurity planning. A CSIRT serves as a centralized authority to report and analyze security issues within an organization. A CSIRT may also recommend potential solutions to the threats and publicize known threats, vulnerabilities, and solutions generally or to a specific information-sharing community. The CSIRT works with hardware and software vendors to obtain information about vulnerabilities and potential solutions. Additionally, coordinating response and recovery efforts with the SWIC and other IT 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 ensure continuity: route diversity, redundancy, and protective/restorative measures. Performing physical and cyber resiliency assessments can assist an organization in ensuring continuity of service in the event of an emergency, justifying network operations and improvement funding requests, increasing organizational control, and prioritizing 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 (RF) best practice implementation plays a critical role throughout the life cycle of a system. RF coverage testing and analysis should be used to define and refine system coverage requirements, supplement baseline coverage studies, Coverage Acceptance Testing, provide in-building coverage measurement including assistance in locating interfering signals, and assist with system optimization as well as ongoing maintenance. Ongoing resiliency assessments should account for the entire system lifecycle, including testing and maintenance.

Goal 3 – Training, Exercises, and Evaluations: Develop and deliver training, exercise, and evaluation programs that target gaps in all available emergency communications technologies

Objective 3.1: Update and ensure the availability of training and exercises 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, and continuity of communications

The development of standardized communications-focused objectives and evaluation criteria for training and exercise programs require thorough understanding of existing gaps across 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 organizations offer training classes and exercises across multiple agencies & jurisdictions whenever possible

Training and exercise programs help identify and mitigate communications challenges, but only if these programs tackle interoperability across the emergency communications ecosystem. Comprehensive programs address technology, process, and human factors related to interoperability; not only an agency's or entity's systems but those of partners, with a focus on where those systems intersect. The capability gaps and interoperability challenges faced by the ecosystem can be incorporated into objectives, injects, and scenarios. Where possible, partners from across the entire ecosystem should be invited to attend as participants, staff, or observers. Serving as evaluation staff is a good way for partners to enhance each other's programs. . 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, region, or Tribe.

Public safety organizations coordinate training and technical assistance across the 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. SWICs have an understanding of training and technical assistance requirements within states and territories. SWICs also assist local, tribal, and individual organizations to participate in training and technical assistance opportunities. Where training requirements cannot be fulfilled with in-state resources, SWICs coordinate and identify training resources with the state training authority (e.g., the 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 system 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, such as quality exercise evaluation guides (EEGs), any facilitator 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; leading to improved trainings, exercises, and capabilities on all sides. Written agreements as to who shoulders costs related to these shared resources are beneficial to support continued use of third party evaluators, controller, and trainers.

Public safety organizations integrate private sector, NGOs, 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. Currently, only 7 percent of public safety organizations report training with NGOs and private-sector entities. In contrast, 23 percent report not training with any other types of organizations, with the rest of organizations falling somewhere in between these extremes. NGOs and private sector entities operate critical infrastructure that provides or supports emergency communications including operations centers, towers, generators, repeaters, and vehicles. Many NGOs 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, NGOs such as 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, NGOs, 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 ECPC 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 ECPC 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, data, and video 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 PSAPs and EOCs. Information flow, volume, and sources of data are all evolving, so training programs need to address the use of new technologies and the impact of change on responders and the work they do. For example, video messaging changes the interaction of a dispatcher with a caller from a voice interaction to a face-to-face interaction. Physical reactions of the dispatcher such as facial expressions are no longer hidden from the distressed caller, necessitating a new set of skills and coping mechanisms for the dispatcher. In the field, body-worn cameras are another change for responders where training is necessary. Administratively, the changes that come with new technologies may require trainings for new approaches to screening and interviewing new 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 implementing NG911 utilize resources and tools to address the impact of incident images/videos on dispatchers

New technologies bring responders not on-scene even 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 (i.e., voice, video, 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 ESF-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

During emergencies and planned events, ESF-2 and communications support personnel are typically required. In order to meet demand, there needs to be adequate training available to allow new personnel to be trained and for 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 NCSWIC develop training curriculums for additional positions within the Information Technology Service Unit

Incident AARs 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 ICS 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 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 and active use of the NIMS doctrine

Success Indicators

Public safety organizations possess primary, secondary, and backup communications capabilities aligned with NIMS and ICS and share appropriate forms (e.g., ICS 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 NIMS and ICS 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, like all other response attributes must scale 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 the confirmation and determination of 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 Public Safety Answering Points (PSAP) and Public Safety Communications Centers (PSCC), 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 (IC) or Incident Management Team (IMT) should remain well-informed about the status of all available operable and interoperable communications capabilities, information that is easily obtained through sharing appropriate ICS form(s).

Public safety organizations assess and improve the timeliness of notification, activation, and response of communications systems providers to support the IC and IMT requirements at incidents and planned events

Anecdotal trends indicate that public safety organizations, of all disciplines, are committing larger complements of 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 IC and IMT 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. Recognizing the importance of the inclusion of communications systems providers, public safety organizations and IC/IMT personnel must be cognizant and comfortable of the expected timelines to acquire 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. It is incumbent upon public safety organizations to ensure sufficient primary, secondary, and backup communications capabilities are available to scale quickly to effectively support and facilitate the transition of a planned event to 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 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. The following are activities recommended to achieve this objective.

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 and other organizations who may provide or receive automatic aid, mutual aid, or share infrastructure or resources or participate in planned events. This sharing of active, available features, functionality, and capabilities of current communications capabilities 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, SOPs, tactical response directives, and/or tactical interoperability communications plans (TICPs) 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, and 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. The doctrine can be essential in completing necessary ICS 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, utilities) in incidents and planned events

As an enhancement to communications coordination public safety organizations should evaluate existing communications policy, 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.

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 NIMS-aligned SOPs 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 SOPs cover NG911; 18 percent cover broadband; 18 percent cover priority services; and 16 percent cover cybersecurity. Clear and effective SOPs enable personnel from across the Ecosystem to successfully coordinate for planned events and unplanned incidents. Additionally, SOPs with mission- or capability-specific roles require coordination across agencies to standardize procedures in the event of an incident requiring cross-jurisdictional response.

NIMS includes communications tactical requirements and resources in the incident action plan (IAP). Incident Command System (ICS) 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 ICS Form 205 is important, sharing the IAP, 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 IAPs ahead of time so that adjustments can be made in a timely manner. Even when operational periods are short and IAPs are produced quickly, planning personnel must work with Communications Unit personnel to ensure resources are distributed appropriately and all section chiefs ensure the IAP 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 developed on the use of personal devices (e.g., bring your own device [BYOD]) based on applicable laws and regulations

The proliferation of personal mobile devices and implementation of network policies, such as BYOD, 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 (MDM) solutions that address configuration management, software patches, audio/video permissions, device-level intrusion detection and prevention, and digital asset management systems, such as a "sandbox" or "virtual desktop". Working with vendors to develop mission-related use cases and requirements

to inform comprehensive MDM solutions can also improve implementation of these solutions. DHS' Mobile Device Adoption Best Practices Guide provides introductory best practices when considering mobile device use, though organizational-level guidance should be in compliance with applicable laws and regulations. In addition, BYOD 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 SOPs

Real-world events, whether planned or unplanned, provide opportunities to translate SOPs 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 assets. Processes developed to test the use of existing or new technologies may be exercised during scenarios, leading to SOP resolution prior to real events. Agencies develop after-action reports (AARs) following events to assist with defining gaps or missing information resolved through the development or revision of SOPs.

Public safety organizations periodically review the priority service programs (e.g., Telecommunications Service Priority, Government Emergency Telecommunications Service, and Wireless Priority Service) to which they subscribe and ensure they have SOPs governing the programs' use, execution, and testing

Government Emergency Telecommunications Service (GETS) provides emergency access and priority processing on the local and long-distance portions of the Public Switched Telephone Network (PSTN) for national security and/or emergency preparedness (NS/EP) users. Wireless Priority Service (WPS) provides NS/EP personnel priority access on wireless networks. The Telecommunications Service Priority (TSP) Program managed by Priority Telecommunications Service gives NS/EP users priority processing of their telecommunications service requests in the event of service disruption. Employing these services can improve continuity of communications.

Public safety organizations periodically test 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 lack of proficiency, established by set minimum standards, in the use of communications capabilities drive appropriate recommendations for modifications and expansion of user instructional documentation, informal and formal trainings, drills, exercises, and SOPs.

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 end-users of any failures or unavailability of a communications feature, function, or capability.

PSAPs, PSCCs, and Emergency Operations Centers (EOCs) address systems and staffing to support communications COOP planning

As part of COOP planning, PSAPs, PSCCs, and EOCs should address staffing requirements and technical resources to support their ability to maintain communications and functions during incidents. This includes succession as well as backup procedures for major systems, such as computer-aided dispatch, radio, and power supply. In addition, PSAPs, PSCCs, and EOCs COOP planning should incorporate relevant capabilities and assets, such as the Telecommunicator Emergency Response Task Forces initiative. Telecommunicator Emergency Response Task Forces can help states 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 NCSWIC**, in coordination with the ECPC, **develop best practices to encourage active network sharing and regionalization of shared services

SAFECOM and the NCSWIC's Shared Communications Systems and Infrastructure (SCSI) focuses on creating the plans, processes, and structures to enhance communications operability, interoperability, security, and continuity throughout the Nation. Benefits of network sharing include 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 NCSWIC identify public safety technology and infrastructure capability gaps

Public safety communications benefit from a validated national perspective on capability gaps. SAFECOM and the NCSWIC identify capability gaps that impact the operability, interoperability, and security of public safety communications. SAFECOM and the NCSWIC provide the capability gaps to ECPC, which address how they can be met through existing technology, technological research and development, and/or marketplace innovation. SAFECOM and the NCSWIC ensure capability gaps collected are also addressed through governance, standard operating procedures, training and exercise guidance and usage/testing advancements.

The ECPC coordinates federal research, development, testing, and evaluation priorities and processes

With organizations often facing common technology challenges, the ECPC can help coordinate these activities by maintaining a database of research and development (R&D) projects on its Federal Emergency Communications R&D Portal, through conducting joint initiatives and assessments, and by driving multi-agency participation in testing programs. ECPC coordinates with:

- Research centers and laboratories that develop and test new communications technologies
- Organizations conducting R&D to address DHS Component requirements and that partner with other public safety organizations to extend this research to meet their needs
- 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.

The ECPC cultivates sustained engagement (e.g., conferences, summits, cooperative agreements) between federal research, development, testing and evaluation programs, such as DHS Science and Technology Directorate and the National Institute of Standards and Technology (NIST) Public Safety Communications Research Division (PSCR), and public safety organizations focused on resiliency, interoperability, and other challenges

With limited resources, state, local, territorial, and tribal organizations are often limited in their ability to develop new technologies. Through its 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 ECPC Working Groups and the SAFECOM Technology Policy Committee to ensure that federal programs are meeting and reflecting a broad cross-section of stakeholder concerns. Also, ECPC encourages federal programs to regularly engage through conferences, summits, pilot projects and cooperative agreements, such as that performed by organizations such as DHS Science and Technology Directorate and NIST PSCR. The ECPC has increased cross collaboration with PSCR on initiatives related to resiliency and capacity building to further identify critical communications technology gaps. Increased ECPC interaction with industry and stakeholders (e.g., communications and IT sector-specific councils and information sharing and analysis centers [ISAC], 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 entire community.

The ECPC partners with the private sector to cultivate 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 R&D is important to technology development, private industry plays a critical role by innovating and developing systems, devices, and applications for the public safety market. Including private industry is essential to the success of any strategy for coordinating the direction of research and development into new capabilities, and public safety organizations have several 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, and 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. Federal departments and organizations 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 standards development organizations to ensure requirements are incorporated into emerging technology—greatly reducing future costs and re-engineering challenges.

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

Success Indicators

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

The results of R&D, 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 NCSWIC 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 NCSWIC guide standards-based LMR evolution

The Project 25 (P25) suite of standards for LMR support interoperability and communications continuity for the public safety community. SAFECOM and the NCSWIC continue to encourage organizations purchasing P25 communications equipment to use the resources made available by P25 Compliance Assessment Program and continue to support P25 standards development for interoperability. DHS, as the senior federal partner in the P25 standards development process and the chair of the P25 Steering Committee, continues to help drive interoperability testing, the addition of enhanced security features, and support for future communications capabilities such as P25 to LTE interfaces.

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

The FirstNet Authority has responsibility to ensure 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 local, state, tribal, and federal 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 needs and assist public safety entities in understanding 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 NG911

The Department of Transportation National Highway Traffic Safety Administration's 911 Program Office plays an active role in coordinating and contributing to 911 policy, standards, and technology development through its work with public safety organizations across the country. The office coordinates with the Federal Communications Commission (FCC), which promotes enhanced and NG911 through its role as a regulator (e.g., Task Force on Optimal PSAP Architecture) and administers the 911 Grant Program. It also provides strategic planning for collection and use of nationwide 911 data and guidance for interstate implementation of NG911. The National 911 Program Office and SAFECOM and the NCSWIC have partnered on the promotion of consistent terminology and assessment of NG9-1 maturity, as well as guidance on Cyber Risks to Next Generation 911 Systems. DoT also chairs the Next Generation 9-1-1- Working Group within the ECPC, which is working to complete a report which inventories federal PSAP and PSCC assets across the US.

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 (EDXL), National Information Exchange Model (NIEM), Structured Threat Information eXpression/Trusted Automated eXchange of Indicator Information (STIX/TAXII), and Global Reference Architecture (GRA). 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. In addition, public safety organizations should enable the interoperability of evolving technologies (e,g., FirstNet, NG911) 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

Acquisition of standards-based infrastructure in a multi-vendor environment supported by compliance testing minimizes the risk of operability and interoperability challenges. Standards-based infrastructure also 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, when crafting 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 NCSWIC publish best practices and updated guidance on standard operating procedures to assist the public safety community in meeting 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 SOPs. 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 NCSWIC 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 Cybersecurity Framework

The NIST 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 THIRA and SPR requirements. Ideally, organizations using the Framework and THIRA/SPR 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 use the Critical Infrastructure Cyber Community Voluntary Program (C³ Voluntary Program)

The C³ Voluntary Program is a public-private partnership aligning business enterprises, as well as local, state, territorial, tribal, and federal departments and agencies in the Emergency Services Sector to existing resources to assist their efforts in using the NIST Cybersecurity Framework. The C³ Voluntary Program, and its implementation guidance, aims to simplify the process for all organizations in the Emergency Services Sector— regardless of their size, cybersecurity risk, or current level of cybersecurity sophistication—to apply the principles and best practices of risk management. Ultimately, the NIST Cybersecurity Framework and C³ Voluntary Program are focused on helping individual organizations reduce and better manage their cybersecurity risks, contributing to a more secure and resilient sector overall.

Objective 6.2: Mitigate cybersecurity vulnerabilities

Success Indicators

SAFECOM and the NCSWIC share planning and mitigation guidance regarding known threats and vulnerabilities

In addition to promoting US-CERT and other Information Sharing Environment notifications of public safety-specific threats and attacks, SAFECOM and the NCSWIC guidance educates the community on known threats and their mitigations. For example, SAFECOM and the NCSWIC guidance regarding RF interference, or "jamming": (1) educates and trains personnel to identify and respond appropriately to RF interference; (2) familiarizes organizations with how to report incidents of RF interference to the FCC and other appropriate authorities; and (3) helps legislators and regulators understand the value of enforcement legislation. Depending on the threat, guidance could also encourage risk mitigation through 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, as well as identify areas for necessary R&D.

Public safety organizations implement interoperable encryption, as needed

Voice and data encryption are increasing in use 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[2]. Guidance on encryption and key management is available to the community, such as the Best Practices for Public Safety Interoperable Communications.[3]

[2] 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 FCC regulations and comply with an approved regional communications plan.

[3] NPSTC'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 FCC regulations and comply with an approved regional communications plan. NPSTC Report: Best Practices for Public Safety Interoperable Communications, May 2018.

SAFECOM and the NCSWIC refine the NG911 Emergency Communications Center (EC3) concept

NG911 networks introduce new vectors for attack that can disrupt or disable operations. As such, the Federal Communications Commission's Task Force on Optimal PSAP Architecture has recommended the implementation of EC3s.[4,5] EC3s 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 EC3 cybersecurity layer for the NG911 architecture will play a vital part in the operation and maintenance of NG911. SAFECOM and the NCSWIC's expertise is vital to refining fundamental attributes of EC3, including governance, funding, usage, operating procedures, technical capabilities, technical architecture, and interconnection requirements. The EC3 layer must provide defined value for PSAPs—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.

NIST evaluates 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 a comprehensive review of the 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. Evaluations may include supply and repair chain risk management, as well as deployment, operations and maintenance guidance. NIST should review protocol standards, as well as provide cybersecurity testing and certification activities, for the public safety community.

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

Success Indicators

NIST establishes 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 NIST should work to develop a plan for setting, testing, and maintaining cyber minimum standards to assist cybersecurity-eligible grant programs in distributing necessary funding to public safety stakeholders. 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' ability to communicate over the past five years. Yet, almost half of respondents had not instituted cybersecurity best practices, such as risk assessment, 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 assists emergency response organizations and policy makers to plan and implement interoperability solutions for data and voice communications.

[4] FCC Task Force on Optimal PSAP Architecture, Adopted Final Report. 29 Jan 2016, https://transition.fcc.gov/pshs/911/TFOPA/TFOPA_FINALReport_012916.pdf

[5] FCC Task Force on Optimal PSAP Architecture, Optimal Cybersecurity Approach for PSAPs, 2 December 2016, https://transition.fcc.gov/pshs/911/TFOPA/TFOPA_WG1_Supplemental_Report-120216.pdf

SAFECOM and the NCSWIC 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

There are voluntary, non-binding, and no cost cybersecurity services available from the Federal Government to the SLTT community, as detailed in the DHS Cybersecurity Services Catalog for SLTT. In addition, public safety organizations may leverage Homeland Security Grant Program (HSGP) State Homeland Security Program (SHSP) and/or Urban Area Security Initiative (UASI) grants for their cybersecurity risk management. The 911 Grant Program might also provide funds for cybersecurity solutions as part of broader operation of NG911 systems.

National Risk Management Center provides a cost study of public safety cybersecurity risk management and evaluates the need for additional grant programs

Eighty percent of state CIO's surveyed in the 2016 National Association of State Chief Information Officers (NASCIO) study indicated lack of sufficient funding as their primary challenge in cybersecurity, and according to the 2018 Nationwide Communications Baseline Assessment, most organizations (81–84 percent) have no funding or insufficient funding for cybersecurity. Targeted grant programs may be necessary to enable public safety organizations' investment in cybersecurity, including foundational security architecture, advanced protective tools, and experienced technical professionals to manage them.

NIST provides incentives for cybersecurity-specific R&D 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. PSCR incentives may include grant programs, pilot programs, hackathons, or other activities. PSCR may collaborate with SAFECOM and the NCSWIC, the National Public Safety Telecommunications Council, and the FirstNet Authority to identify and develop cybersecurity requirements. Additional collaboration with US-CERT, NCCIC, and others will help PSCR to collect and prioritize known cyber threats for research and development.

Appendix 1. Requirements Matrix

Table A1-1. 6 U.S.C. § 572 Requirements Cross-referenced with 2019 NECP Content

2019 NECP Section	S.C. § 572 Requirement Filled
Section 1.0 - Introduction	6 U.S.C. § 572(a)-(b) 6 U.S.C. § 572(c)(7) 6 U.S.C. § 572(c)(10)
Section 2.0 – Emergency Communications Ecosystem	6 U.S.C. § 572(b)(1)-(2) 6 U.S.C. § 572(c)(3) 6 U.S.C. § 572(c)(5)
Section 3.0 – NECP Strategic Goals	6 U.S.C. § 572(c)
• *Goal 1*	6 U.S.C. § 572(b) 6 U.S.C. § 572(c)(5)-(7) 6 U.S.C. § 572(c)(9)
• *Goal 2*	6 U.S.C. § 572(c)(1) 6 U.S.C. § 572(c)(4) 6 U.S.C. § 572(c)(7)
• *Goal 3*	6 U.S.C. § 572(a)(1)-(2) 6 U.S.C. § 572(c)(3) 6 U.S.C. § 572(c)(5)-(6) 6 U.S.C. § 572(c)(8)
• *Goal 4*	6 U.S.C. § 572(a)(1)-(2) 6 U.S.C. § 572(c)(2) 6 U.S.C. § 572(c)(4)-(6) 6 U.S.C. § 572(c)(9)
• *Goal 5*	6 U.S.C. § 572(a)(1)-(2) 6 U.S.C. § 572(c)(1)-(6) 6 U.S.C. § 572(c)(8)
• *Goal 6*	6 U.S.C. § 572(a)(1)-(2) 6 U.S.C. § 572(c)(1)-(2) 6 U.S.C. § 572(c)(8)
4.0 - Implementation	6 U.S.C. § 572(c) 6 U.S.C. § 572(c)(10)
5.0 - Conclusion	6 U.S.C. § 572(c) 6 U.S.C. § 572(c)(8)

Appendix 2. Key Authorities

Statutory Authorities

This appendix lists key authorities that guide the development, implementation, and management of the National Emergency Communications Plan (NECP). For example, *Title XVIII of the Department of Homeland Security (DHS) Appropriations Act of 2007* impacts the NECP directly by requiring DHS to periodically update the plan.[6] In addition, related statutes pertaining to emergency communications nationwide also indirectly help to guide NECP improvements and revisions. This list identifies the foundation of 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. 93-288 (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

Tables A2-2 to A2-5 describe 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 (HSPD) –5, Management of Domestic Incident* (2003)
2. *Homeland Security Presidential Directive 7—Critical Infrastructure Identification, Prioritization, and Protection.* (2003)
3. *Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors* (2004)
4. *Homeland Security Presidential Directive (HSPD) 20 – National Continuity policy* (2004)
5. *National Security Presidential Directive (NSPD) 51/Homeland Security Presidential Directive 20, National Continuity Policy* (2007)
6. *National Security Decision Directive 97—National Security Telecommunications Policy,* (1983)
7. *National Security Presidential Directive 39 – U.S. Space-Based Position, Navigation, and Timing Policy* (2004)
8. *Presidential Policy Directive (PPD) – 8, National Preparedness,* (2011)
9. *PPD – 21, Critical Infrastructure Security and Resilience,* (2013)
10. *PDD – 4: National Space Policy* (2007)
11. *PDD – 41: U.S. Cyber Incident Coordination* (2016)

[6] 6 U.S.C. § 572. NECP (2007).

12. *Executive Order (E.O) 13175 – Consultation and Coordination with Indian Tribal* (2000)
13. *E.O. 13407 – Integrated Public Alert and Warning System* (2006)
14. *E.O. 13618 – Assignment of National Security and Emergency Preparedness Communications Functions* (2012)
15. *E.O. 13616 – Accelerating Broadband Infrastructure Deployment* (2012)
16. *E.O. 13636 – Improving Critical Infrastructure Cybersecurity* (2013)

Related Authorities

While Tables A2-1 to A2-5 include primary authorities that most directly impact emergency communications, Table A2-6 lists other homeland security policy, plans, and doctrine that influence the NECP development and implementation lifecycle and that the NECP, in turn, helps to accomplish.

1. *National Preparedness System* (2011)
2. *National Infrastructure Protection Plan (NIPP)* – NIPP 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)

Appendix 3. 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. 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 both the emergency response community and the affected populations, as well as with other governmental entities.

Local Jurisdictions

Local leaders, emergency managers, and public safety officials prepare their communities to manage incidents locally. Among their numerous responsibilities, these officials provide strategic guidance, manage resources, develop and implement policies and budgets, and oversee local preparedness efforts to improve emergency management and response capabilities. A number of 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 Public Safety Communications 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. 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. A listing of the key statewide officials and governing bodies with responsibility for emergency communications are described below. This list is not intended to be exhaustive as some states have additional agencies or individuals with whom they interact.[7]

- **Statewide Interoperability Coordinator.** The Statewide Interoperability Coordinator, or SWIC, 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.

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

- **State Single Point of Contact.** The Single Point of Contact, or SPOC, serves as the coordinator for the State and Local Implementation Grant Program and First Responder Network Authority efforts with respect to the 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, 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, as well as 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 each state, territorial governments are also responsible for coordinating the emergency communications resources needed to respond to incidents of all types and any scale, determining their resource capacity, and ensuring an efficient process for requesting assistance, when necessary. Given that their geographical locations often present unique challenges for receiving assistance during times of disaster, it is equally important for territorial governments to prioritize emergency communications. It is especially critical for territories to build relationships and partnerships among neighboring islands, other nearby countries, states, the private sector, nongovernmental organizations, and the Federal Government.

Tribal Nations

Tribal Nations are geographically dispersed across the United States, and tribe size varies 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 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.

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; and
- Supporting federal, state, local, tribal, and territorial operational efforts, providing surge capacity and coordinating distribution of federal resources to support emergency communications.

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

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 network restoration during outages and service failures and support 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 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 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 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 Nationwide Public Safety Broadband Network. Its expertise 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 provide 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.[8] Nongovernmental organizations include voluntary and non-profit organizations that provide shelter, food, and other essential support services and disaster relief.[9] As technology evolves, NGOs 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 community emergency response teams and 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 of any scale.

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:

[8] For a list of all core capabilities, refer to the *National Preparedness Goal*, www.fema.gov/ppd8.
[9] FEMA. *National Response Framework*, June 2016, pg. 9. https://www.fema.gov/media-library-data/1466014682982-9bcf8245ba4c60c120aa915abe74e15d/National_Response_Framework3rd.pdf.

- **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 Groups 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 FCC 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.

- **National Council of Statewide Interoperability Coordinators.** Comprised of all Statewide Interoperability Coordinators (SWICs), the National Council of Statewide Interoperability Coordinators assists SWICs 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/Emergency Preparedness.** Committee in July 2012 as a forum—comprised of representatives from at least eight designated Federal agencies—to recommend policy and advise the President on national security and emergency preparedness communications issues.

- **Communications Executive Committee.** Executive Order 13618, Assignment of National Security and Emergency Preparedness Communications Functions, established the National Security and Emergency Preparedness Executive.

- **National Security Telecommunications Advisory Committee.** The President's National Security Telecommunications Advisory Committee (NSTAC) is composed of private sector executives who represent major communications and network service providers, as well as information technology, finance, and aerospace companies. Through DHS, NSTAC 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 40 representatives from various public safety organizations that are part of the DHS SAFECOM program.

- **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 (FEMA) regions. Each Regional Emergency Communications Coordination Working Group has unique membership dependent on regional government structure and processes.

- **SAFECOM.** SAFECOM is an emergency communications program of the 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.

Appendix 4. 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. 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) Emergency Communications Division has used the Interoperability Continuum to develop the priorities and measure the goals of the NECP. For more information, see Section 4.0 *Implementing the NECP*.

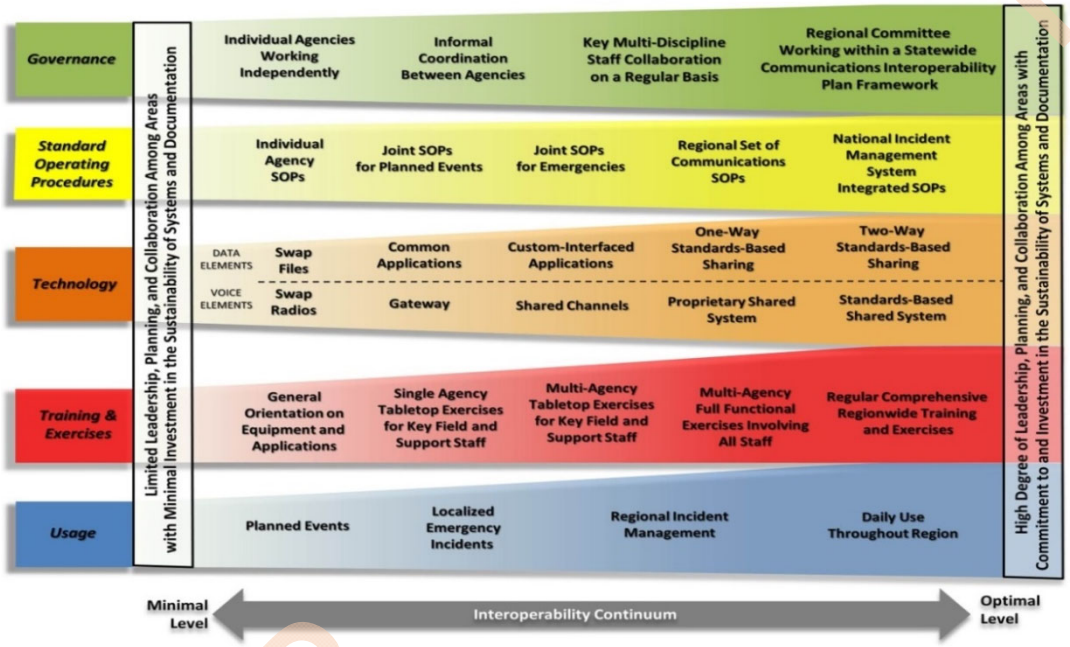


Exhibit A5-1. SAFECOM Interoperability Continuum

Interoperability is a multi-dimensional challenge. To gain a true 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, local, and tribal agencies.

Appendix 5. Source Documents

This appendix lists the key source documents that the Department of Homeland Security (DHS) used to inform and shape the concepts, goals, and objectives of the 2019 NECP. This list is not exhaustive; rather, it highlights the primary source documents that were developed since the 2014 NECP.

Federal Departments and Agencies

1. DHS/FEMA: Comprehensive Preparedness Guide (CPG) 201: *Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR)* Guide 2018 https://www.fema.gov/media-library/assets/documents/165308
2. DHS/CISA ECD: FY 2018 SAFECOM Guidance on Emergency Communications Grants https://www.dhs.gov/safecom/blog/2018/05/16/release-fy-2018-safecom-guidance-emergency-communications-grants
3. National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (2018): https://www.nist.gov/cyberframework
4. DHS Cybersecurity Services Catalog for SLTT (2018): https://www.us-cert.gov/sites/default/files/c3vp/sltt/SLTT_Hands_On_Support.pdf
5. DHS/FEMA: National Incident Management System (2017) https://www.fema.gov/national-incident-management-system
6. DHS/FEMA: National Preparedness Report (2017) https://www.fema.gov/national-preparedness-report
7. DHS/FEMA: National Response Framework, Third Edition https://www.fema.gov/national-preparedness-report
8. National Institute of Standards and Technology: Project 25 Compliance Assessment Program https://www.nist.gov/ctl/pscr/newsroom/press/p25-cap
9. Federal Communications Commission Task Force on Optimal Public Safety Answering Point Architecture (2015-2016) https://www.fcc.gov/about-fcc/advisory-committees/general/task-force-optimal-public-safety-answering-point
10. United States National Grid Recommendations for update of the NECP
11. National 911 Program Office: Guidelines for State NG911 Legislative Language (2018) https://www.911.gov/pdf/Guidelines_for_State_NG911_Legislative_Language.pdf

Congressional Panels, Testimonies, and Reports

1. Written Testimony of Rear Admiral Ronald Hewitt, USCG (Retired) Assistant Director for Emergency Communications, CISA: 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. National Emergency Management Association Biennial Report, 2018
2. Via Satellite: First Responder's Guide to Satellite Communications, 2018
3. 2017 Joint Meeting of the Major Cities Chiefs Association's Technology and FirstNet: Workshop on Law Enforcement Priorities and Recommendations for FirstNet
4. NPSTC Report Best Practices for Public Safety Interoperable Communications: Best Practices 2018
5. Using Future Broadband Communications Technologies to Strengthen Law Enforcement, RAND

Appendix 6. 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 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.

All Hazards Incident Dispatch Team (IDT)

Specially trained communications personnel who are certified in tactical, wildland, and urban-interference incidents. The IDT responds to large scale events and incidents and work 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

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, to provide a basis for decision-making.

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 (AUXCOMM)

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 (RBIS) 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; 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 (LTE). Broadband and LTE 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 all 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 (COMC)

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 (COML) and helps with such tasks as assigning equipment, frequencies, and following up on and keeping track of the status of orders. The COMC determines the extent and availability of communications coordination possible for a given incident.

Communications Duty Officer (CDO)

Similar to the Communications Coordinator (COMC), 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 (COML).

Communications Unit Leader (COML)

The COML heads the communications unit and is responsible for integrating communications. The COML designs, orders, manages, and ensures the installation and maintenance of all communications systems. The COML must be familiar with Incident Command Systems (ICS) 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 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 2013: 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.

Dispatch Center

Agency or interagency dispatch centers, 911 call centers (e.g., public safety answering points), emergency control or command dispatch centers, or any naming convention given to the facility and staff that handles emergency calls from the public and communication with emergency management/response personnel.

Emergency Communications

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

Emergency Communications Ecosystem

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

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

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 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.

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. HSEEP 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 (INCM)

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

Incident Communications Center (ICC)

An established location close to an Incident Command Post (ICP) 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, designed to aid in the management of resources during incidents. It is used for all kinds of emergencies and is applicable to small and large, complex incidents. 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 (COML) and Incident Commander Staff to determine IT resource requirements to support incident objectives such as developing Information Management Plan (manage data sharing); determining and ordering needed personnel, equipment, and services; and supervising IT and Communications Help Desk.

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, and shared system or channels).

Internet of Things (IoT)

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

MsgR

Message Runners, (MsgRs) physically relay messages to areas not yet served with any communications system

NECP

The *Homeland Security Act of 2002*, as amended, requires DHS to develop the NECP; the Plan 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, local, tribal, and territorial governments; private sector entities; and the public, allies, and other nations.

Network Decommissioning

The process of removing systems and equipment from active service.

Next Generation 911

Next Generation 911 services" means a secure, IP-based, open-standards system comprised of hardware, software, data, and operational policies and procedures that:
(A) provides standardized interfaces from emergency call and message services to support emergency communications;
(B) processes all types of emergency calls, including voice, text, data, and multimedia information;
(C) acquires and integrates additional emergency call data useful to call routing and handling;
(D) delivers the emergency calls, messages, and data to the appropriate public safety answering point and other appropriate emergency entities based on the location of the caller;
(E) supports data, video, and other communications needs for coordinated incident response and management; and
(F) interoperates with services and networks used by first responders to facilitate emergency response.
(source: NENA master glossary - definition agreed upon by NG911NOW Coalition - NASNA, NENA and iCERT)

Nongovernmental Organization

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.

NGOs/Private Sector

Non-profit or for-profit organizations participating in public safety/emergency communications planning, use or reconstitution (e.g., Non-Governmental Organizations [NGOs], utilities, communication service providers, equipment operators, transportation, food distribution, Volunteer Organizations Active in Disasters [VOAD]).

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., fire, law enforcement) 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 (PTB)

Primary tool for observing and evaluating the performance of Incident Command System (ICS) 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 (TSP) Program. Authorizes priority services for domestic telecommunications services (e.g., Government Emergency Telecommunications Service [GETS] and Wireless Priority Service [WPS]).

Private Sector Entity

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

Project 25

(P25 or APCO-25) is 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, P25 fills the same role as the European Terrestrial Trunked Radio (TETRA) 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 theTelecommunications Service Priority, enable rapid restoration if services are damaged or destroyed.

Public Safety Entity

An entity that provides public safety services and 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).

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 Public Safety Communications Center.

Radio Operator (RADO)

Staffs the Incident Communications Center (ICC), using radios to receive information and relay messages.

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.

State Preparedness Review

Required by several DHS grants, the THIRA process helps communities understand threats and hazards their varying impacts. The THIRA process results in community-informed capability targets and resource requirements necessary to address anticipated and unanticipated risks.[1] https://www.fema.gov/media-library/assets/documents/165308

Strategic Planning

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 Communications 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, 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.*

Tactical Dispatcher

Supports Communications Unit staff with accurate and timely documentation of events during high-risk operations, special events and major incidents in which a command post is activated.

Tactical Dispatch Team (TDT)

Provide on-site communications support during incidents or planned events. The TDT provides support to the Incident Commander with accurate and timely documentation of events during a planned events and unplanned incidents.

Technical Assistance

Support to state, local, tribal, and territorial 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 NS/EP organizations to receive priority treatment for vital voice and data circuits or other telecommunications services. See https://www.dhs.gov/telecommunications-service-priority-tsp.

Threat and Hazard Identification and Risk Assessment

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

THSP

Technical Specialists (THSP) is a catch-all term for outside specialists providing expertise to the Communications Unit Leader (COML) including amateur radio, computer network technicians, and satellite communications (SATCOM).

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 (NS/EP) cell phone users, (e.g., senior members of the Presidential administration, local emergency managers, fire, and police chiefs, and technicians in wireline and wireless carriers, banking, nuclear facilities, and other vital national infrastructures). See https://www.dhs.gov/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, local, tribal, and territorial governmental partners in order to foster better coordination and working relationships

Appendix 7. Acronyms

5G	Fifth Generation
AVL	Automatic Vehicle Location
C³	Critical Infrastructure Cyber Community Voluntary Program
CAD	Computer Aided Dispatch
CAT	Coverage Acceptance Testing
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
COOP	Continuity of Operations
CSIRT	Computer Security Incident Response Team
DHS	Department of Homeland Security
EC3	Emergency Communications Center n
ECPC	Emergency Communications Preparedness Center
EDXL	Emergency Data EXchange Language
EMS	Emergency Medical Services
EOC	Emergency Operations Centers
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
GIS	Geographic Information System
GRA	Global Reference Architecture
HSEEP	Homeland Security Exercise and Evaluation Program
HSGP	Homeland Security Grant Program
IAP	Incident Action Plan
ICAM	Identity, Credential, and Access Management
ICE	U.S. Immigration and Customs Enforcement
IoT	Internet of Things
IP	Internet Protocol
IPAWS	Integrated Public Alert and Warning System
IRT	Incident Response Teams
ISE	Information Sharing Environment
IT	Information Technology
JWPMO	Joint Wireless Program Management Office
LMR	Land Mobile Radio
LTE	Long-Term Evolution
MAA	Mutual Aid Agreements
MCPTT	Mission Critical Push-to-Talk
MOA	Memoranda of Agreement
MOU	Memoranda of Understanding
NCCIC	National Cybersecurity and Communications Integration Center
NCSWIC	National Council of Statewide Interoperability Coordinators
NECP	National Emergency Communications Plan
NGO	Nongovernmental Organization
NG911	Next Generation 911
NHTSA	National Highway Traffic Safety Administration
NIEM	National Information Exchange Model
NIMS	National Incident Management System
NIST	National Institute of Standards and Technology
NPSTC	National Public Safety Telecommunications Council
OASIS	Organization for the Advancement of Structured Information Standards
P25	Project 25
PSAP	Public Safety Answering Points
PSCC	Public Safety Communications

		Centers
PSCR		Public Safety Communications Research Program
PSRC		Public Safety Research Center
R&D		Research and Development
RAN		Radio Access Network
RF		Radio Frequency
RICP		Regional Interoperable Communications Plans
SAA		State Administrative Agency
SDO		Standard Development Organizations
SHSP		State Homeland Security Program
SIEC		Statewide Interoperability Executive Committees
SIGB		Statewide Interoperability Governing Bodies
SOP		Standard Operating Procedure
SPR		Stakeholder Preparedness Review
SPR		State Preparedness Review