Emergency Communications Preparedness Center: Annual Strategic Assessment

Calendar Year 2019 Report to Congress

May 27, 2021

Homeland Security

Cybersecurity and Infrastructure Security Agency (CISA)

Message from the Director

On behalf of the Cybersecurity and Infrastructure Security Agency (CISA) Emergency Communications Preparedness Center (ECPC), I am pleased to submit to Congress the 2019 Annual Strategic Assessment (ASA).

Congress authorized the establishment of the ECPC in 2009, which serves as the federal focal point for interoperable and operable communications coordination. The ECPC works to address gaps in emergency communications and enables emergency response providers and relevant government officials to continue to communicate in the event of natural disasters, public health emergencies, acts of terrorism, other man-made incidents, and planned events.

Collectively, the ECPC has made substantial progress to build collaboration and coordination across federal departments and agencies. Individual federal departments and agencies themselves have also made strides to organize and strengthen their own emergency communications programs. This report aims to identify and prioritize where further action is needed to improve interoperability.

This document has been compiled pursuant to 6 U.S.C. § 576. The report assesses federal coordination efforts toward improving the continuity and interoperability of communications in key areas found in the goals and priorities of the 2019 National Emergency Communications Plan (NECP), to include: (1) Governance and Leadership; (2) Planning and Procedures; (3) Training, Exercises, and Evaluation; (4) Communications Coordination; (5) Technology and Infrastructure; and (6) Cybersecurity. For each of these elements of effective public safety communications, the ECPC identified common challenges and priorities, as well as successes. As this assessment is based on actions taken in 2019, it does not explore communications activities undertaken in response to the COVID-19 pandemic. COVID-19 activities and the communications lessons learned from the pandemic response will be covered thoroughly in the report for calendar year 2020.

Pursuant to congressional requirements, this report is provided to the following Members of Congress:

The Honorable Bennie Thompson
Chairman, House Committee on Homeland Security

The Honorable John Katko
Ranking Member, House Committee on Homeland Security

The Honorable Frank Pallone, Jr.
Chairman, House Committee on Energy and Commerce

The Honorable Cathy McMorris Rodgers

Ranking Member, House Committee on Energy and Commerce

The Honorable Gary C. Peters
Chairman, Senate Committee on Homeland Security and Government Affairs

The Honorable Rob Portman
Ranking Member, Senate Committee on Homeland Security and Government Affairs

The Honorable Maria Cantwell
Chairwoman, Senate Committee on Commerce, Science, and Transportation

The Honorable Roger Wicker
Ranking Member, Senate Committee on Commerce, Science, and Transportation

Sincerely,

Brandon Wales
Acting Director
Cybersecurity and Infrastructure Security Agency

Executive Summary

The Emergency Communications Preparedness Center (ECPC) was established by 6 U.S.C. § 576 to improve interoperable and operable communications coordination among federal departments and agencies. The ECPC is composed of 14 federal departments and agencies who meet regularly to address gaps in emergency responders' abilities to communicate across jurisdictions and functions. Pursuant to the authorizing statute, the ECPC developed the Annual Strategic Assessment (ASA) to assess federal interoperability with appropriate partner agencies and the impact of coordination on continuity of communications and interoperability during day-to-day operations and emergency incident response.

Reliable and interoperable communications capabilities are critical to enabling federal, state, local, tribal, and territorial (FSLTT) public safety and national security/emergency preparedness (NS/EP) personnel to operate during steady-state and emergencies. Doing so allows responders to maintain situational awareness, coordinate response efforts, and share mission-critical information. The Federal Government plays a key role in addressing challenges and improving the effectiveness of emergency communications. Collectively, FSLTT agencies have a responsibility to coordinate efforts to enhance interoperability, reduce costs, and strengthen and maintain relationships with agencies from all levels of government.

The ASA examines progress on federal coordination efforts defined by the six goals of the 2019 National Emergency Communications Plan (NECP), including: (1) Governance and Leadership; (2) Planning and Procedures; (3) Training, Exercises, and Evaluation; (4) Communications Coordination; (5) Technology and Infrastructure; and (6) Cybersecurity.

Each section of this assessment focuses on common challenges, successes, and next steps needed to move closer to accomplishing each goal of the 2019 NECP. The 2019 ASA documents communications efforts during coordinated large-scale disasters, planned events, routine public safety communications operations, and trainings and exercises that tested the interoperability of federal departments and agencies. The ASA analyzes the successes, challenges, and lessons learned from those events. The ASA reflects current federal priorities for improving emergency communications, identifies progress made by the Federal Government against the 2019 opportunities, and outlines opportunities for further federal coordination in the years ahead.

In 2019, the ECPC found federal departments and agencies were continuing to make progress in establishing interoperable communications, while maintaining legacy systems that support department- and component-level operable communications. Departments and agencies approached interoperable communications from multiple angles, including:

- Strengthening governance structures, increasing interoperability coordination between components, and streamlining the administration of communications programs;
- Employing novel funding mechanisms to plan for future interoperability projects and applying lessons learned to increase continuity of communications during emergency events;
- Identifying training and exercise needs, including standardized training, assessment, and testing criteria;

- Continuing to scope the use of the National Incident Management System (NIMS) for their unique missions and partnerships for sharing communications infrastructure;
- Exploring partnerships to increase emerging communications capabilities, such as Next Generation 911 (NG911), and leveraging real-world events to demonstrate the positive impact of interoperability projects;
- Identifying cybersecurity gaps in communications systems, such as information sharing between partners and enhanced training requirements.

More information on these key findings can be found in Section III. Summary of 2019 ASA Findings and Recommendations.

2019 Annual Strategic Assessment

Table of Contents

I. Statutory Language

6 U.S.C. § 576[1] sets forward the following provisions:

> *(c) FUNCTIONS: The Center shall--*
>
> *(1) Serve as the focal point for interagency efforts and as a clearinghouse with respect to all relevant intergovernmental information to support and promote (including specifically by working to avoid duplication, hindrances, and counteractive efforts among the participating federal departments and agencies)—*
>
> *a. The ability of emergency response providers and relevant government officials to continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters; and*
>
> *b. Interoperable emergency communications;*
>
> *(2) Prepare and submit to Congress, on an annual basis, a strategic assessment regarding the coordination efforts of federal departments and agencies to advance—*
>
> *a. The ability of emergency response providers and relevant government officials to continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters; and*
>
> *b. Interoperable emergency communications;*
>
> *(3) Consider, in preparing the strategic assessment under paragraph (2), the goals stated in the National Emergency Communications Plan under Section 572 of this title; and*
>
> *(4) Perform such other functions as are provided in the Emergency Communications Preparedness Center (ECPC) Charter described in subsection (b) (1).*

The 2019 Annual Strategic Assessment (ASA) meets the statutory requirements outlined in 6 U.S.C. § 576. This assessment provides information on federal coordination efforts and documents the impact coordination has on interoperability and the ability of public safety response providers to continue to communicate in the event of natural disasters, acts of terrorism, other man-made disasters, and planned events. The ECPC leveraged principles from the 2019 National Emergency Communications Plan (NECP) and the SAFECOM Interoperability Continuum to develop the 2019 ASA. This report is intended to provide Congress with a strategic assessment of federal coordination efforts and actions for the ECPC to address this year.

[1] 6 U.S.C. § 576 sets forth the establishment, operation, and function of the Emergency Communications Preparedness Center (ECPC)

II. Scope and Methodology

As the administrator of the ECPC, CISA developed the 2019 ASA in coordination with federal member departments and agencies.[2] The following section describes the ASA scope, data collection approach, analysis process, and procedures for reviewing department and agency-specific emergency communications profiles. The ASA evaluates improvements in federal emergency communications and federal coordination, highlighting capabilities that support emergency preparedness and response activities. By compiling best practices and lessons learned, this assessment serves as a resource to enable federal, state, local, tribal, and territorial (FSLTT) departments and agencies to enhance continuity and interoperability across the Emergency Communications Ecosystem.[3]

Scope and Analytical Framework

The ASA details activities from the 2019 calendar year, including planned events (e.g., the nationwide emergency alert system [EAS] test), federal programs, exercises, investments, and responses to disasters. The 2019 ASA findings align to the 2019 NECP goals and the SAFECOM Interoperability Continuum,[4] providing a common framework for identifying challenges, trends, and lessons learned.

Data Collection Approach

In 2019, CISA outlined a new data-gathering strategy to conduct a more efficient cross-agency analysis of interoperable communications and identify common themes between participants. CISA brought together 14 federal departments and agencies[5] for a one-day workshop on March 4, 2020, at the Smithsonian National Museum of the American Indian in Washington, D.C. The workshop design included facilitator led-large group discussions, small breakout discussions on functional topics, targeted departmental interviews, and polling activities. This format enabled CISA to efficiently collect 825 discrete interview responses through interviews and small group discussions, as well as develop collective recommendations regarding emergency communications successes, challenges, and capabilities aligned to the six goals of the 2019 NECP. Federal departments and agencies provided input to their Federal Profiles (i.e., comprehensive summaries of their organization's emergency communications offices, functions,

[2] The terms agency/agencies and department/departments are used interchangeably, and include federal departments, independent agencies, and agencies within or subject to the review by another agency of the U.S. Government. The terms are consistent with the definitions in 5 U.S.C. § 551 and §§ 104, 105 (to include independent authorities).

[3] The various functions and people that exchange information prior to, during, and after incidents and planned events, including, traditional emergency responder disciplines, medical facilities, utilities, nongovernmental organizations, the media, and private citizens

[4] CISA, Interoperability Continuum: A Tool for Improving Emergency Response Communications and Interoperability. 2014. https://www.cisa.gov/publication/interoperability

[5] 14 federal departments and agencies participated in the ASA process, however, due to unforeseen circumstances, two departments were unable to attend the ASA workshop. Follow-up interviews were conducted to collect relevant data.

policies, programs, resources, points of contact, and responsibilities reserved for internal, ECPC use only). In order to collect individual data points, CISA:

- **Held individual departmental interviews:** CISA tailored approximately 50 questions to individual departments and agencies and gathered detailed information on 2019 emergency communications challenges and successes at the department level, aligned to the 2019 NECP strategic goals.

- **Gathered functional subject matter data:** During small group interagency discussions, 36 workshop participants provided input based on their individual functional expertise, including areas such as continuity of communications, Emergency Support Functions, telecommunications and radio management, policy formation across interoperable communications capabilities (e.g., cybersecurity, emerging technologies, governance), alerts and warnings, Next Generation 911 (NG911), strategic planning, and partnerships and coordination. This workshop format allowed information -sharing regarding successes and challenges encountered in 2019 and yielded informative discussions between participants.

- **Conducted follow-up outreach and interviews:** After the workshop, CISA conducted follow-up activities to ensure information was collected from all ECPC member departments and agencies. CISA conducted a follow-up interview with representatives from the Federal Communications Commission (FCC) who were unable to attend the workshop. CISA also provided the interview questions to the Department of Health and Human Services (HHS) to fill out and return since their representatives were unable to attend the workshop due to HHS's role in the ongoing COVID-19 pandemic response. Additionally, CISA conducted targeted outreach to select departments and agencies to gain clarity on interview and small group discussions, which enabled a more thorough data collection process. Additional outreach was also needed to complete and verify the department-specific Federal Profiles.

Immediately following the workshop, CISA collected feedback from the 36 workshop participants regarding their experience, which was generally positive. Most participants noted they greatly enjoyed to opportunity to hear the experiences of their colleagues from other departments and agencies. To improve the experience, participants suggested more time was needed at future workshops to discuss topics and build relationships and expressed a desire to bring additional personnel from their department or agency in the coming years. CISA concluded data collection for the 2019 ASA in May 2020.

Data Analysis Approach

In support of the 2019 ASA, CISA gathered extensive qualitative notes from department and agency interviews, workshop activities, and follow-up outreach and interviews. CISA utilized the workshop data to assess federal successes towards achieving the NECP goals and recognize potential areas for improvement.

II. Summary of 2019 ASA Findings and Recommendations

The following tables provide a summary of the 2019 ASA findings and recommendations, structured by 2019 NECP goals.

Table 1: 2019 ASA Key Findings

2019 ASA Key Findings	
Section	**Key Finding**
Governance and Leadership	Federal departments and agencies continued to face challenges coordinating interoperable communications policy between internal components due to insufficient coordinating bodies and other institutional barriers
	Senior leaders frequently struggled to accurately assess and direct public safety communications investments without a dedicated budget line item
Planning and Procedures	Federal departments and agencies benefited from up-to-date communications plans during exercises and real-world incident responses
	Department-wide alignment of communications planning and procedures promoted unity of effort in achieving communications goals
Training, Testing, and Exercises	Federal departments and agencies with strong communications training and exercise programs supported dedicated staff to coordinate training activities
	Geographically based and hazard-specific exercises accurately simulated response environments, enabling federal departments and agencies to identify communications gaps
	Annual exercises with a communications-focus grew in popularity to compensate for limited regular exercise opportunities
	Federal departments and agencies successfully coordinated testing, training, and exercises with state and local authorities, particularly for alerts, warnings, and notifications capabilities
Communications Coordination	Incompatible equipment between responders inhibited effective communications coordination during incident response and exercises
	Interagency collaboration during steady-state operations increased communications interoperability for planned and unplanned events
Technology and Infrastructure	Federal departments and agencies began to establish NG911 capabilities but faced many governance, planning, and stakeholder coordination challenges
	Formal agreements with state and local partners improved communications interoperability, clarifying how external partners can securely access shared infrastructure

2019 ASA Key Findings

Section	Key Finding
Cybersecurity	Federal departments and agencies addressed cybersecurity gaps in communications systems, including upgrading radio cyber protections and improving training
	Federal departments and agencies undertook initiatives to improve internal and external cybersecurity information sharing, increasing coordination with partner organizations
	Federal departments and agencies required all employees to take cybersecurity training, providing a broad awareness of common cybersecurity incidents

Table 2: 2019 ASA Recommendations

2019 ASA Recommendations

Section	Recommendation
Governance and Leadership	Establish an organization-wide nexus within departments/agencies for interoperability policy, resourcing, and systems decision-making, bringing together all internal stakeholders
	Consider highlighting public safety communications funds in department/agency budgets and establish interoperability-focused forums for senior leaders
Planning and Procedures	Explore establishing sufficient funding vehicles for shared emergency communications projects
	Develop procedures to maintain continuity of operations following administrative changes, personnel departures, or other circumstances
	Establish and adhere to set timelines for developing, implementing, and reviewing communications plans and asset lifecycle plans
Training, Testing, and Exercises	Standardize communications response training at a federal level
	Develop and implement emergency communications performance metrics to assess responder and operator needs
	Ensure emergency communications technicians are properly trained across the Federal Government
Communications Coordination	Apply National Incident Management System typing uniformly to communications-specific training and assets across their organizations
	Explore partnerships for infrastructure sharing with other external partners that address roles, responsibilities, liabilities, spectrum, infrastructure, data interoperability, and data sharing

2019 ASA Recommendations	
Section	**Recommendation**
Technology and Infrastructure	Work in concert with external partners to develop NG911 capabilities, identifying opportunities to share systems and infrastructure to reduce funding challenges
	Conduct periodic gap analyses of major communication systems, leveraging detailed and actionable data to justify requests for resources
Cybersecurity	Emphasize cybersecurity awareness, cultivate cybersecurity information sharing, and improve information sharing governance bodies
	Share guidance and best practices for implementing cybersecurity into public safety communications infrastructure
	Implement additional cybersecurity training on how to protect public safety communications equipment and infrastructure

IV. Analysis

The 2019 ASA examined major events, thirteen communications disciplines impacting continuity of communications and interoperability, and the six 2019 NECP strategic goals, including**: (1) Governance and Leadership; (2) Planning and Procedures; (3) Training, Exercises and Evaluation (4) Communications Coordination; (5) Technology and Infrastructure; and (6) Cybersecurity**. The following pages contain a summary of findings and spotlight successes and challenges in federal emergency communications coordination.

Emergency Communications Defined

The means and methods for exchanging information necessary for successful incident management[6]

Governance and Leadership

Governance and Leadership Defined

Coordination and decision-making processes that guide interoperable communications priorities and policy[7]

NECP Goal 1: Governance and Leadership

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

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

Objective 1.2: Structure more inclusive governance by expanding membership composition

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

In 2019, federal partners faced challenges coordinating interoperability policy between components, as well as overcoming administrative barriers. Federal departments and agencies continued to make progress towards recommendations of previous ASAs, particularly establishing centralized communications governance bodies, as well as streamlining administrative processes to better prioritize communications resources.

Challenges and Priorities

Inconsistent Intra-Agency Governance

Emergency communications governance remained inconsistent across

[6] CISA, 2019 National Emergency Communications Plan. 2019. https://www.cisa.gov/publication/2019-national-emergency-communications-plan

[7] CISA, 2019 National Emergency Communications Plan. 2019. https://www.cisa.gov/publication/2019-national-emergency-communications-plan

departments and agencies, ranging from foundational (i.e., components independently coordinate communications decisions) to more mature models (i.e., components employ a central coordinating body). The majority of departments and agencies reported that they did not have a mechanism to coordinate interoperable communications decisions across their components. Rather, components independently prioritized communications interoperability policy and resources.

Even when intra-agency governance bodies exist, institutional barriers may prevent effective coordination. For example, the Department of Justice (DOJ) reviewed the communications-related policy and funding requests through the Wireless Communications Board (WCB). The WCB convened stakeholders from across DOJ to review communications policy and funding allocations. While the WCB successfully integrated DOJ components into a collaborative decision-making body for communications projects, only one DOJ component provided funding for intra-agency projects. DOJ representatives noted this can slow the approval process as departmental leadership must reconcile component requests with available resources.

Similarly, the Department of Homeland Security (DHS) Joint Wireless Program Management Office (JWPMO) supported DHS components when acquiring communications systems. According to DHS, JWPMO's support ensures components coordinate to procure interoperable communications equipment, eliminating technical barriers to future interoperability projects. Despite success supporting equipment acquisitions, the JWPMO is currently without authority to coordinate other aspects of interoperable communications projects, such as policy and shared infrastructure decisions. This narrow focus on acquisition limited JWPMO's ability to foster interoperability between DHS components. Participants noted DHS components may benefit from a governance body that convenes stakeholders from across the department, providing holistic coordination for interoperable communications policy.

The ECPC developed the Federal Emergency Communications Governance Guide in 2019, recognizing that effective governance structures empower federal departments and agencies to construct solutions for operable, interoperable, and continuous emergency communications and better address resource, staffing, technological, and operational capabilities and needs. This document outlines seven principles that provide a framework to address emergency communications interoperability, operability, and continuity challenges by a) improving resource coordination, b) developing more holistic partnerships, and c) enhancing collaborative efforts.

Federal Emergency Communications Governance Guide Principles

1. Reinforce a holistic approach that includes a variety of partner organizations
2. Provide advisory functions that enable authorities, structures, and processes to support interoperability policy development and decision-making
3. Identify the dynamics of meetings, engagements, and plans to ensure continued stakeholder involvement and improved management
4. Adapt federal governance as mission needs expand and evolve
5. Share critical information and assets across key stakeholders to improve awareness of policies and interoperability challenges
6. Share public safety NS/EP communications systems
7. Design networks that build upon collaborative requirements, which meet each participating agency's unique needs

Administrative Barriers to Intra-Agency Governance

In addition to inconsistent governance approaches, federal departments and agencies noted administrative processes might prevent leadership from conducting an accurate assessment of interoperable emergency communications investments. For example, federal departments and agencies noted budgets often do not have a separate line item for public safety communications, complicating efforts to prioritize funding for interoperability projects. According to the Department of Defense (DOD), each service branch frequently combines emergency communications funding with other business functions (e.g., information technology) when allocating resources. Similarly, the Department of the Interior (DOI) noted its budgeting process does not separate emergency communications funding into discreet line items. For example, in 2019, the DOI Bureau of Land Management's communications programs drew funding from several sources, including wildland firefighting, mineral, land, and realty budgets. Without dedicated funding line items, departmental leadership from DOD and DOI experienced challenges measuring the amount of funding needed to support interoperable communications projects. In turn, this prevented departments and agencies from determining which resources support emergency communications, measuring emergency communications resource needs, and prioritizing resources for interoperability projects.

Successes

Progress Towards Building Strong Governance Models

In 2019, federal departments and agencies made progress implementing more centralized governance models for emergency communications. DOD began scoping a public safety communications steering group comprised of senior leadership from across the department. This steering group will provide a forum to discuss public safety communications challenges, inform cross-component interoperability decisions, and identify opportunities for cross-component communications projects. To meet a similar goal, in 2019, the United States Department of Agriculture (USDA) reorganized the structure of Chief Information Officers (CIOs) across the department under the OneUSDA initiative. Previously, component CIOs primarily directed communications projects independently. Under the new organizational structure, all component CIOs now report to the department CIO, enabling senior leadership to coordinate communications priorities across the department.

The DOI highlighted the department's successful efforts to establish strong communications governance, illustrating a potential framework for other federal stakeholders to increase inter-component coordination. DOI used the Radio Executive Steering Committee and the Radio Program Management Council to coordinate land mobile radio (LMR) policy and investments across the department. The steering committee is chaired by directors for fire and law enforcement functions, representing two of the largest communications users within the department. Eight DOI bureaus sit on the committee, as well as representatives from the department's safety, budget, and emergency management functions. The committee successfully fostered a collaborative environment to inform interoperability policy and represented field staff needs to senior leadership. Furthermore, in 2019 DOI successfully filled the department's interoperability coordinator position, creating a single point of contact (POC) for all interoperability programming within the department.

Progress Toward Improving Administrative Processes

In 2019, federal departments and agencies undertook initiatives to overcome administrative barriers, paving the way for more effective communications governance. For example, while the Department of Labor's (DOL) components all maintained independent budgets, the department leveraged the Emergency Management Center to pool resources into a shared working capital fund. The capital fund enabled the department to collaboratively identify communications projects supporting interoperability between components (e.g., emergency rescue programs) and streamline funding allocations. Similarly, in 2020 DOD will require service branches to list public safety communications expenditures as a stand-alone budget line item. This change will allow DOD leadership to analyze public safety communications investments across the department and prioritize existing resources to support interoperability projects.

LOOKING AHEAD TO 2020-2025:
Governance and Leadership Recommendations for Federal Departments and Agencies

1. Establish an organization-wide nexus within departments/agencies for interoperability policy, budget, and systems decision-making, bringing together all internal stakeholders
2. Consider accounting for public safety communications funds in department/agency budgets with discreet line items and establish interoperability-focused forums for senior leaders

Planning and Procedures

Planning and Procedures Defined

Formal documents that detail department or agencies interoperable communications objectives, progress indicators, and day-to-day operational processes, plans, and procedures to guide the deployment of resources and technologies[8]

Through structured interviews with federal emergency communications personnel, the ECPC found a lack of consistently developed and updated communications plans and procedures. Where system lifecycle plans exist, it remains difficult for departments and agencies to adhere to the outlined timeframes due to the nature of the federal budget process. The ECPC also found that departments and agencies benefitted during exercises and real-world events in 2019 from consistently keeping plans updated, creating new plans as needed, and consolidating department-wide communications planning procedures.

NECP Goal 2: Planning and Procedures

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

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

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

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

Challenges and Priorities

Inconsistent Use of Communications Planning

Across the Federal Government, there is a lack of consistency in developing and updating communications plans and procedures. For example, the DOJ's Federal Bureau of Investigation (FBI) reported no set schedule for updating such plans. These plans are only updated as needed or when spurred by external forces, such as audits by the Government Accountability Office (GAO) or Office of the Inspector General. Additionally, many other federal departments and agencies lack a central body with the responsibility and/or authority to develop and update emergency communications plans. The FBI noted it could dedicate more time to developing and updating interoperability plans for the DOJ if it had the resources to establish and operate a dedicated interoperability office.

[8] CISA, 2019 National Emergency Communications Plan. 2019. https://www.cisa.gov/publication/2019-national-emergency-communications-plan

Some federal departments and agencies use a decentralized structure for interoperability planning. The United States Coast Guard (USCG) recently implemented a policy directing every unit with communications responsibilities to have an interoperability plan and contingency plan. However, it has delegated planning to the district level. Each USCG district establishes independent memorandums of understanding with state and local agencies, creating risks to coordinated communications planning across the department.

Adherence to Established Lifecycle Plans

Lifecycle planning encompasses the planning, acquisition, implementation, maintenance, refreshment, and disposal of communications systems.[9] However, some federal departments and agencies have not been able to adhere to established lifecycle plans due to decreased funding and the rapidly evolving Emergency Communications Ecosystem.[10] For example, the Department of Transportation (DOT) reported that communications asset upgrades are planned to occur every four years; however, implementation has been inconsistent. Additionally, external forces, such as a procurement freeze, can hinder the implementation of lifecycle plans. DOJ's equipment lifecycle upgrades were hampered by a procurement freeze for the past six years; however, the freeze was recently lifted. During the procurement freeze, DOJ was unable to purchase new equipment to replace outdated assets or perform maintenance on existing equipment. As a result, DOJ could not abide by its lifecycle plan.

Successes

Properly Executing Established Communications Plans

Regularly updated plans assisted with exercises and real-world incident response in 2019. The DOL classified and internal agency communications response plans are updated on a monthly schedule. Similarly, the DOL's continuity plans are reviewed and updated quarterly. Having up-to-date communications plans helped DOL respond to the 2019 Puerto Rico earthquakes. DOL's plans enabled personnel accountability and allowed for quick facility damage assessments. Consistent communications-enabled DOL to assess the need to evacuate personnel and bring in outside assistance or respond with personnel already stationed in Puerto Rico. The USDA's continuity plans are updated at least twice a year, and ad hoc updates also occur whenever significant events or changes arise.

In 2019, the FCC Office of the Managing Director (OMD) Logistics Branch, which oversees the plan for managing FCC-internal communications infrastructure and assets, participated in the Eagle Horizon exercise.[11] The FCC OMD Logistics Branch reported that having plans in place, in coordination with the FCC Operations Center (a central hub for all FCC communications), facilitated testing and validating the reliability of the FCC's communications.

[9] CISA, 2018 Emergency Communications System Lifecycle Planning Guide, 2018. https://www.cisa.gov/safecom/funding

[10] CISA, 2018 Emergency Communications System Lifecycle Planning Guide, 2018. https://www.cisa.gov/safecom/funding

[11] Eagle Horizon is an annual continuity exercise for all federal executive branch departments and agencies to test their Continuity of Operations Plan (COOP) by deploying their Emergency Relocation Groups

Federal continuity of operations plans outline the roles, responsibilities, and procedures required to maintain mission-critical communications in an emergency scenario (e.g., natural disaster, cybersecurity incident). Based on 2018 ASA findings, federal agencies would benefit from regular updates to continuity communications plans to ensure federal stakeholder's emergency procedures account for emerging threats and trends. The majority of departments, such as USDA, planned for and tested the continuity of operations (COOP) plans and procedures in 2019. COOP planning, practices, and theories should remain consistent while leveraging new capabilities to ensure continuity of communications during an emergency event.

Intra-Agency Alignment of Communications Planning and Procedures

Newly developed plans that were implemented in 2019 contributed to the department-wide alignment of communications priorities. For example, the DOD completed the DOD Digital Modernization Strategic Plan. The draft plan, approved by the DOD CIO, will align all public safety communications policy and planning initiatives across DOD components into a department-wide strategy. The DOD anticipates using this strategy to issue new public safety communications-focused directives and instructions. Each service branch independently determines strategic goals and outcomes for their own public safety communications functions, while department-wide directives and instructions provide overall guidance to components and encourage adherence to best practices (e.g., separating public safety communications funding into a discreet budget line item). The consolidated strategy will provide the DOD CIO with the authority to ensure that DOD components comply with department-wide goals.

Additionally, DOJ completed and began implementing a new law enforcement communications strategy. This plan supports increased funding requests from DOJ component agencies and is helping revive the communications governance authority the FBI is standing up on behalf of DOJ. The new plan also enables DOJ to consider alternatives to its current communications systems (e.g., moving from a single system to shared systems with state agencies). While the current plan supports voice communication, it does not support data or video communications.

Likewise, the Department of Energy's (DOE) Emergency Communications Network develops a complete inventory of programmatic documents that reference and define communications policies and procedures for the Department. These policies and procedures are wholly developed to satisfy the governance, oversight, and operational response mission of the DOE.

LOOKING AHEAD TO 2020-2025:
Planning and Procedures Recommendations for Federal Departments and Agencies

1. Explore establishing sufficient funding vehicles for shared emergency communications projects
2. Develop procedures to maintain continuity of operations addressing administrative changes such as personnel departures or other resource limitations
3. Establish and adhere to set timelines for developing, implementing, and reviewing communications plans and asset lifecycle plans

Training, Exercises, and Evaluation

Training, Exercises, and Evaluation Defined

Programs during steady-state operations to improve communications skills, test capabilities, and assess an organization's progress towards interoperability goals[12]

Effective training and exercise programs enable response personnel to successfully execute plans, policies, and procedures governing the use of communications, improve proficiency with communications equipment, and target gaps in communications capabilities. In 2019, federal partners noted strong participation in robust training and exercise programs; however, the need remains for proper evaluation procedures to identify and close gaps.

NECP Goal 3:
Training, Exercises, and Evaluation

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

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

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

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

Challenges and Priorities

Lack of a Federal Standard for Communications Training

Developing and implementing effective training programs improves emergency response capabilities. CISA's Interoperable Communications Technical Assistance Program is funded to provide direct support to state, local, and tribal emergency responders and government officials through the development and delivery of training, tools, and onsite assistance to advance public safety interoperable communications capabilities. However, CISA does not provide this training to federal departments and agencies. Federal partners reported a lack of federally standardized trainings specific to communications equipment and procedures, which is known to inhibit incident response. For example, first responders from different organizations may not use the same terminology or operating procedures for similar equipment, creating barriers to establishing seamless incident communications. While the Federal Emergency Management Agency (FEMA) provides training standards through the NIMS National Qualification System (NQS), participation is voluntary. For instance, DOI components use NQS training criteria for the Communications Unit Leader (COML) position. In 2019, DOI's COML trained personnel supported thousands of wildland fire response operations, ensuring communications staff across

[12] CISA, 2019 National Emergency Communications Plan. 2019. https://www.cisa.gov/publication/2019-national-emergency-communications-plan

the department shared the same terminology and skillsets. Other federal departments and agencies noted NQS communications qualifications are geared heavily towards certain incident types (e.g., wildland fire) and did not fit their department's or agency's mission requirements. As a result, many federal departments and agencies continued to follow proprietary approaches to communications training. Federal departments and agencies expressed interest in establishing a unified all-hazards training requirement system aligned with FEMA's Incident Command System. Establishing federal-wide training standards would reduce operational barriers to interoperability during emergency incidents and promote a shared information environment among first responders.

Inadequate Communications Specific Training and Exercises

Federal departments and agencies value emergency communications trainings and exercises that allow participants to test and evaluate emergency communications interoperability, infrastructure, and personnel capabilities. Consistent participation in planned events strengthens response to unplanned events. Federal departments and agencies noted they appreciate participating in multi-agency trainings and exercises; however, communications-specific injects are often overlooked when developing training and exercise opportunities. For example, DOD mentioned during its multitude of annual exercises in 2019, public safety communications injects were frequently left out. Additionally, the Department of the Treasury (Treasury) noted if a communications technology is not used day-to-day or often enough, it will not be included in training opportunities. The DOJ noted an absence of training for communications operators at the department level and intermittent use of equipment. To mitigate this issue, the ECPC encourages federal departments and agencies to build NIMS practices into all public safety trainings and exercises, such as active shooters, pandemics, and natural disasters, to train relevant responders and staff. 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.

Federal Interoperability Performance Measures

The public safety community can enhance emergency communications through the evaluation of training and exercises. 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."[13] Having this information is crucial to advancing emergency communications. Furthermore, there is no common set of federal benchmarks focused on interoperability that exists for federal departments and agencies to assess the maturity of emergency communications systems across the nation. In 2019, CISA and state partners developed the State Interoperability Markers Program: 25 interoperability markers aligned to the SAFECOM Interoperability Continuum, designed to collect key data about a state's interoperability capabilities to enable states to use data to drive strategic planning, funding, and technical assistance requests. Some federal departments and agencies have already kicked off efforts to implement interoperability performance measures. For example, the FCC has a pending rulemaking exploring whether performance metrics should be adopted to improve the

[13] DHS CISA, 2019 National Emergency Communications Plan. September 2019. https://www.cisa.gov/publication/2019-national-emergency-communications-plan

effectiveness of alerting. If federal partners were to replicate a similar framework development process, either at an inter-agency or intra-agency level, potential Federal Government benefits could include:

- Understanding interoperability capabilities and gaps to assist states, tribes, and territories in choosing impactful Technical Assistance for their needs;
- Responding to Congressional, GAO, and Office of Management and Budget (OMB) requests for CISA program impacts; and,
- Justifying resource requirements to departmental leadership, OMB, Congress, and the President.

Successes

2019 Eagle Horizon

Exercises are essential for ensuring public safety communications capabilities are operable and responders are trained to effectively use capabilities during planned events and incidents. Response and support agencies participate in communications exercises to test available technologies and information sharing tools; identify gaps in capabilities, techniques, and training; and prepare for real emergency incidents. Eagle Horizon is an annual continuity exercise for all federal executive branch departments and agencies to test their COOP by deploying their Emergency Relocation Groups. Eagle Horizon applies scenarios such as hurricanes, improvised nuclear device detonations, earthquakes, and cyber-attacks during the exercise. Federal departments and agencies, such as the FCC, noted Eagle Horizon as an excellent opportunity to test and validate the reliability of communications. During the exercise, HHS observed benefits in having prepared alert notification messages available in the system that enabled personnel to send out preapproved department-wide messages to HHS staff. With the integration of Alerts and Warnings in particular, these geographically based, hazard-specific exercises are best suited to simulate real world challenges and will continue to attract participants year after year.

2019 EAS Nationwide Test

On August 7, 2019, FEMA, in coordination with the FCC, conducted a nationwide test of the EAS. The live test, which uses the hierarchical, broadcast-based distribution system, assesses whether the national EAS would perform as designed if activated and helps to ensure the reliability and effectiveness of broadcast-based alerting as a failsafe to the national emergency communications infrastructure.[14] According to the final report, 82.5% of EAS test participants received the alert successfully. On retransmission, 79.8% of test participants successfully retransmitted the alert. The FCC highlighted in the report that it will continue to take steps to improve the broadcast-based alerting process.

[14] FCC, PSHSB, Report: August 7, 2019 Nationwide EAS Test (2020) https://docs.fcc.gov/public/attachments/DOC-364279A1.pdf.

LOOKING AHEAD TO 2020-2025:

Training, Exercises and Evaluation Recommendations for Federal Departments and Agencies

1. Standardize communications response training at a federal level
2. Develop, implement, and track emergency communications performance metrics to assess responder and operator needs
3. Ensure emergency communications technicians are properly trained across the Federal Government

Communications Coordination

Communications Coordination Defined

Operational processes that enhance interoperable communications during incident response activities[15]

NECP Goal 4: Communications Coordination

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

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

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

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

Objective 4.4: Strengthen resilience and continuity of communications throughout operations

Effective coordination relies on operational processes that enhance interoperable communications during incident response activities. Crucial to effective incident response, communications coordination relies on building interoperability between responders at all levels of government. This involves using NIMS to build a common vocabulary and ensuring communications equipment and systems are compatible with those of other departments and agencies. The ECPC found a lack of consistent use of NIMS among federal departments and agencies and instances of incompatible equipment between responders. However, the ECPC also noted successes in spectrum deconfliction between federal departments and agencies.

Challenges and Priorities

Equipment Incompatibility

The ECPC found that incompatible equipment between responders can inhibit effective communications coordination. In 2019, DOJ reported a challenge with incompatible equipment due to the procurement freeze, which limited the amount of new equipment the DOJ could acquire. Single band radios prevented FBI personnel from talking to agencies/responders on different spectrums. However, the FBI reported the agency used commercial off-the-shelf technology as a stopgap to increase interoperability with partner organizations. Additionally, the FBI noted local law enforcement counterparts often do not understand the importance of encryption, leading to incompatible equipment between federal and local responders. During a

[15] CISA, 2019 National Emergency Communications Plan. 2019. https://www.cisa.gov/publication/2019-national-emergency-communications-plan

JWPMO-sponsored exercise, the USCG identified challenges ensuring FSLTT partners received and applied correct encryption keys. USCG and representatives from the Transportation Security

Administration noted each component independently determines its own process for receiving keys and reprogramming radio equipment. Some components use over-the-air-rekeying to efficiently distribute encryption keys, while others must manually rekey each piece of equipment.

Inconsistent NIMS Implementation

FEMA developed NIMS to enhance coordination among responders at all levels of government. However, the ECPC found a lack of consistency in the application of NIMS across federal departments and agencies. For example, neither the Treasury nor the Department of Commerce (DOC) sponsored any staff for communications-specific NIMS training in 2019. While Treasury and other federal departments use the concept of NIMS typing for communications resources, representatives noted wording is adjusted for department-needs. DOJ does not have an organized department-wide effort to use NIMS typing for communications. The DOJ did report the FBI field offices have COMLs, but training is ad hoc and dependent on each field office's budget. At DHS, the US Secret Service (USSS) does not rely on NIMS qualifications for training and reported they do not have the experience to coordinate using interagency response language.

Communications Systems and Infrastructure Sharing

The ECPC also found challenges still exist with sharing communications systems and infrastructure. Federal departments and agencies operating along the southern and northern borders reported areas with limited operability for public safety agencies at all levels of government. Until voice operability improves, interoperability will continue to suffer due to a lack of access to reliable communications equipment, infrastructure, and services. Interoperability is further challenged by the need for improved encryption services, operational coordination, system coverage, periodic repetitive training, and federal user integration into local, regional, and statewide systems. The USSS and DOI cited difficulty establishing site leases, equipment sharing, and infrastructure sharing as challenges to building shared communications systems. In 2019, departments and agencies noted they encouraged senior leadership to consider rule changes to limit liability, as sharing communications systems and infrastructure has the potential to increase operability and interoperability of emergency communications using fewer resources.

National Incident Management System

NIMS defines the comprehensive approach to allow jurisdictions and organizations at all levels of government to work together to prevent, protect against, mitigate, respond to, and recover from incidents. It provides stakeholders with shared vocabulary, systems, and processes to successfully deliver emergency management capabilities. NIMS can be implemented across three major components—resource management, command and coordination, and communications and information management.

Successes

Spectrum Deconfliction for Planned Events

In 2019, the USSS experienced success with their National Special Security Event (NSSE) spectrum deconfliction group, enabling USSS to identify interoperability issues between FSLTT partners at large-scale planned events. Through the NSSE spectrum deconfliction group, USSS established a common operating language of communications terms between FLSTT organizations, as well as educating partners on LMR interoperability issues during large events. The USSS NSSE spectrum deconfliction group will continue to foster collaboration between a wide variety of FSLTT partners, increasing interoperability for unplanned events.

LOOKING AHEAD TO 2020-2025:

Communications Coordination Recommendations for Federal Departments and Agencies

1. Apply National Incident Management System typing uniformly to communications-specific training and assets across their organizations
2. Identify and pursue partnerships for infrastructure sharing with other external partners that address roles, responsibilities, liabilities, spectrum, infrastructure, data interoperability, and data sharing

Technology and Infrastructure

Technology and Infrastructure Defined

Assets and equipment that support interoperability between different organizations, leverage partner resources for shared projects, and promote standards-based systems[16]

Technology and infrastructure can foster interoperability between different organizations, help leverage partner resources for shared projects, and promote standards-based systems. In 2019, federal departments and agencies continued to advance interoperability between 911 systems and explored ways to build new communications capabilities while sustaining legacy systems.

NECP 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

Challenges and Priorities

NG911 Implementation

Federal departments and agencies continued to explore NG911 applications and implementation strategies tailored to federal requirements. 911 services are a critical component to emergency response, connecting emergency services directly with communities and gathering vital information for first responders. Legacy 911 systems primarily rely on voice communications technologies, while NG911 systems can support enhanced data collection and sharing capabilities (e.g., multimedia, enhanced location services). A key advantage of NG911 services is enhanced location services, enabling dispatchers to gather and share more specific location data from the public. This enables first responders to more quickly and accurately respond to emergency incidents.

Federal NG911 capabilities continue to develop but face risks related to governance, planning, and implementation challenges. In 2019, DOD, in conjunction with SLTT partners, began initiatives to prepare for the department's transition to NG911. DOD noted SLTT partners' NG911 capabilities varied substantially depending on the jurisdiction, presenting interoperability challenges for DOD facilities that rely on SLTT partners to support emergency response.

[16] CISA, 2019 National Emergency Communications Plan. 2019. https://www.cisa.gov/publication/2019-national-emergency-communications-plan

Departments and agencies noted these uncertainties hindered federal partners from undertaking the technical planning required for NG911 adoption.

In 2019, DOD noted federal partners may have unique technical challenges, related to location data, which could impact NG911 capabilities. For example, U.S. Navy installations usually do not use fixed street addresses for building locations but instead rely on a numbering system. The U.S. Navy's current 911 infrastructure cannot quickly share location information with first responders; DOD personnel must escort first responders to an emergency incident within DOD facilities. In 2019, the U.S. Navy began employing geographic information systems to geotag buildings on base. Geotagging buildings resolves a key technical hurdle for providing enhanced location services, enabling the DOD to take advantage of future NG911 capabilities.

Building vs. Sustaining Communications Capabilities

Federal departments and agencies must frequently prioritize resources between sustaining legacy communications systems or building new capabilities. Federal partners may leverage findings from real-world incidents or exercises to communicate the value of interoperability projects to decision-makers. Across the Federal Government, there exists a variety of LMR, long-term evolution (LTE), and LMR-LTE integrated capabilities. As agencies continue to maintain LMR services and adopt LTE broadband, LMR and LTE integrated solutions offer the potential to bridge users and improve communications across departmental and jurisdictional lines. While LMR systems provide robust voice services, they are not designed to carry large amounts of data traffic in conjunction with these voice services. Although not widely used, there are opportunities for low-speed data capability using LMR systems (e.g., a status button on an LMR radio that indicates personnel are on scene or global positioning system location data) to populate an application or service hosted on the LTE system. Additionally, there are several types of dual use devices that support an LTE network—one subscriber unit with an LMR radio and LTE radio—but the interactions do not cross over and remain LMR to LMR and LTE to LTE.

Treasury uses LTE for COOP and to communicate between components. Several Treasury components use an LMR-LTE integrated system paired with a commercial subscription-based provider, which connects department-provided cell phones to radio systems. This LMR-LTE integrated system allows an individual on a cell phone to transmit voice and low-speed data to an individual using an LMR system.

The DOI National Park Service uses LTE-based technology to monitor portions of the southwest border of the United States. LTE networks enable a sensor monitoring system that detects movement and captures photos of individuals engaged in unauthorized activities near the border. The system sends a message with the individual's photo to a communications center, which can then relay it to U.S. Customs and Border Protection, United States Border Patrol, and local law enforcement. DOI also uses LTE cellular device capabilities to remotely monitor systems' functionality and maintenance to better identify necessary repairs at these sites.

The DOT Federal Aviation Administration (FAA) uses LTE smartphones as default devices for individual user communications, while LMR radios are primarily used in poor coverage areas and during emergency situations to complement FAA's LTE technologies. Currently, the FAA is looking into procuring new technologies that allow LMR radios and LTE cell phones to communicate via the same device, thereby eliminating the need to carry two devices.

Successes

DOD Sharing Infrastructure and Systems with SLTT Partners

In 2019, DOD noted facilities may opt for a variety of solutions to support the NG911 transition, including sharing SLTT 911 infrastructure, matching SLTT NG911 investments, or incorporating technical changes to support future NG911 capabilities. For example, a DOD study noted the Shaw Airforce Base 911 center, located in Charleston, South Carolina, regularly experienced a low call volume. In 2019 the DOD negotiated a memorandum of understanding (MOU) with the City of Charleston to take over emergency call and dispatch services for Shaw Airforce Base. This transition allowed local partners to provide service to the DOD installation while reducing DOD's overhead cost for maintaining a discreet 911 center. This shared infrastructure project reduced DOD's future costs, enabling DOD to utilize NG911 capabilities when SLTT partners transition to NG911 systems. Sharing infrastructure also aligned the DOD facility with SLTT partner governance and planning decisions, increasing interoperability between partner organizations.

In 2019, DOD coordinated with the State of California to ensure interoperability with the State's transition to NG911 services. DOD began planning to upgrade 911 infrastructure at select facilities to match SLTT capabilities, ensuring interconnectivity with statewide data sharing systems. Working with California stakeholders, DOD noted SLTT partners may elect to charge additional fees to maintain interoperability between NG911 and legacy 911 infrastructure. DOD reported that the potential responsibility to pay for the upkeep of SLTT legacy 911 systems will encourage some facilities to match SLTT NG911 infrastructure and capability investments, enhancing the ability to share emergency response data with SLTT partners moving forward.

Applying Lessons Learned to Support Interoperability Projects

Following an emergency incident at the White House in 2015, the USSS identified challenges with the agency's communications systems, including coverage, end-of-lifecycle equipment, and limited interoperability with SLTT partners. Since 2000, the USSS maintained a legacy LMR network in the National Capital Region (NCR), which reached the end of its lifecycle. The legacy network did not extend beyond the NCR, even though in 2019, the USSS frequently operated in the New York City urban area.

Using lessons learned, the USSS successfully lobbied decision-makers for additional resources to close specific communications gaps. Additional resources enabled the USSS to sustain their legacy LMR network while building new capabilities, such as Radio over Internet Protocol service. The upgraded LMR system also enabled the USSS to reassess coverage in the NCR to fit mission needs, introduce additional resiliency features, and expand capabilities to the New York City urban area. Due to limited communications resources, USSS leadership prioritized maintaining the legacy network to support mission critical voice services at the expense of equipment and infrastructure improvements. However, in 2019, the USSS began negotiating formal MOUs with SLTT partners, outlining roles and responsibilities for utilizing the new LMR system. Formal MOUs will enable USSS to increase interoperability with SLTT partners during emergency incidents, which USSS noted was a limited capability on previous LMR systems.

LOOKING AHEAD TO 2020-2025:
Technology and Infrastructure Recommendations for Federal Departments and Agencies

1. Work in concert with external partners to develop NG911 capabilities, identifying opportunities to share systems and infrastructure to reduce funding challenges
2. Conduct periodic gap analyses of major communication systems, leveraging detailed and actionable data to justify requests for resources

Cybersecurity

Cybersecurity Defined

The prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability. Includes the protection and restoration (when needed) of information networks and wireline, wireless, satellite, public safety answering points, and 911 communications systems and control systems[17]

While emergency communications have typically been focused on radio communications, the evolution of voice communications systems and the increasing use of data and video systems requires a closer examination of the cybersecurity vulnerabilities of communications systems. The NECP included Cybersecurity as a strategic goal in 2019 for the public safety community to better prepare for cyber incidents and continually evolve security requirements in coordination with partners in their Emergency Communications Ecosystem. CISA serves as the cybersecurity lead for all federal civilian executive branch departments and agencies operating on the .gov domain, providing policy and technical assistance and advocating for cybersecurity services and resources.

NECP 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

Challenges and Priorities

Complex Threat Environment

Federal departments and agencies continue to take individual approaches to addressing cybersecurity gaps; a holistic approach can better recognize and address cyber vulnerabilities across the Federal Government. Malicious actors may disrupt communications through a wide variety of means, including physically tampering with communications infrastructure (e.g., radio towers), network hardware (e.g., routers), or end-user devices (e.g., radio handsets). They may deploy malicious software to compromise networks, disrupt operations, or steal information (e.g., ransomware, advanced persistent threats), or conduct social engineering (e.g., phishing) to trick authorized personnel into providing system access and/or credentials. In 2019, cyber-

[17] CISA, 2019 National Emergency Communications Plan. 2019. https://www.cisa.gov/publication/2019-national-emergency-communications-plan

attacks severely disrupted response capabilities of local jurisdictions. For example, several county sheriff's departments in the Southern United States were attacked with ransomware that infiltrated through a remote desktop. Additionally, a major metropolitan police department fingerprint database was hacked due to a single compromised communication device.

Federal departments and agencies are urged to follow CISA Cyber Essentials guidelines[18] to achieve a holistic approach to mitigate cybersecurity threats. This approach includes developing security awareness and vigilance through cybersecurity training, protecting critical assets and applications through inventories, establishing regular backups, and building system redundancies to ensure availability. Federal departments and agencies should maintain inventories of devices and hardware in use across their organization to know which assets are at risk. In addition, public safety organizations should continue to implement employee awareness trainings aimed at simple cyber hygiene practices to help employees understand their role in cybersecurity and how the actions they take help keep organizations secure. In 2019, federal departments and agencies had variable approaches to cybersecurity, each employing their own cybersecurity infrastructure, networking, and training requirements. Few departments and agencies indicated use of the National Institute of Standards and Technology (NIST) Cybersecurity Framework, or similar standards, to provide a minimum set of cybersecurity capabilities across their department or agency. The NIST Framework, in collaboration with private sector partners, enhances existing risk management processes and helps owners and operators of critical infrastructure identify, assess, and manage cyber risks within their organizations.

Cybersecurity Incident Information Sharing

Information sharing is fundamental to preparing for cyber incidents and the public safety community must continually work together, both internal and external to their department or agency, to identify cyber risk and advance security requirements. Information sharing about key cyber threats and vulnerabilities remains mixed among federal departments and agencies. In 2019, departments and agencies noted even when information sharing mechanisms exist, such as Security Operations Centers (SOCs), they may not meet the department or agency's cybersecurity needs. A SOC is a centralized unit that manages security issues on an organizational and technical level. In 2019, the Department of State (DOS) and DOT both noted internal cybersecurity information sharing as a key issue. At DOT, the SOC does not have the ability to receive classified information, making cybersecurity threat information sharing difficult. The FAA constitutes three-quarters of the department but does not share cybersecurity information with the SOC. While this has been a challenge in recent years, the Director of the SOC is working to address this problem by hosting intelligence briefings to share cyber threats and incidents across the department. In addition, DOS reported that their cybersecurity and policy staff did not frequently share information and that separately operated coordination activities.

Federal departments and agencies should continue to enhance internal information sharing by establishing interdepartmental and agency POCs to aggregate and report or share critical cybersecurity threats. This will develop a greater culture of cyber awareness within the

[18] CISA, Cyber Essentials. 2019. https://www.cisa.gov/publication/cisa-cyber-essentials

department or agency and reduce cybersecurity vulnerabilities through improved policies on information sharing within organizations. Today, more than ever, there is a need to foster and promote a culture of sharing cyberthreat intelligence across all levels of government, the private sector, nongovernmental organizations, and the public.

Successes

Improving Federal Communications Cybersecurity

In 2019, federal departments and agencies made progress towards closing cybersecurity gaps in communications systems, including upgrading LMR cyber protections and improving training programs. DOI noted a significant challenge had been synchronizing LMR security controls, which include access control, identification and authentication, system and communication protection, and system information and integrity between LMR users and information technology (IT) personnel. The USDA solved this issue by creating an LMR package that provides controls for other systems to leverage. This eases the burden on IT personnel to meet those controls while ensuring redundant capabilities are met. The USDA tailored security controls and security control inheritance models[19], defined responsibilities, and held each office accountable via a pre-arranged agreement.

Cybersecurity Training Enhancements

Enterprise IT cybersecurity training is essential for developing effective organizational cybersecurity knowledge and behavior. During the 2019 ASA Workshop, every department and agency reported that cybersecurity training requirements were in place for all employees, providing a broad awareness of common cybersecurity incidents (e.g., phishing). Most cybersecurity trainings included instructions on how to secure equipment, properly protect proprietary data, and prevent personnel from falling victim to phishing scams. For example, DOC requires additional training for individuals that click on internal test phishing emails. These types of trainings are vital to keeping federal departments and agencies secure as cybersecurity incidents occur daily across the public safety landscape. There is a strong need for continued training to mitigate cybersecurity risks, especially amongst those focused on protecting communications infrastructure and equipment.

Collaborative Information Sharing Tools

As the federal lead, CISA is responsible for the cybersecurity of all federal civilian executive branch departments and agencies, i.e., those departments and agencies on the ".gov" domain. CISA works with departments and agencies to address new and existing challenges, such as cloud computing and mobile technology risks, through such programs as the National Cybersecurity Protection System (EINSTEIN), Cyber Directives, Continuous Diagnostics and Mitigation, and others. In 2019, federal departments and agencies undertook initiatives to improve cybersecurity information sharing internally and increase coordination with partner organizations, such as establishing centralized coordination points for cybersecurity services and participating in inter-agency working groups. These information hubs, channels, and standards

[19] A specific system or application receives protection under the tailored security controls

improved coordination and information sharing on best practices at the federal level. Departments and agencies reported that it is beneficial to establish a single cybersecurity POC as the position allows for centralized coordinated cybersecurity information sharing across components, similar to Statewide Interoperability Coordinators. This position helps reduce cybersecurity vulnerabilities through improved policies on information sharing enterprise wide.

The FCC's Communications Security, Reliability, and Interoperability Council (CSRIC) brings together FSLTT and private-sector stakeholders to provide recommendations regarding ways to ensure security, reliability, and interoperability of communications systems. The Council focuses on a range of public safety and homeland security-related communications matters and provides recommendations to the FCC, regarding the security and reliability of communications systems, including telecommunications, media, and public safety. In 2019, CSRIC VII released a report to improve interoperability of legacy 911 and NG911 systems, entitled *The Current State of Interoperability for 911 Systems.*[20] The report explores the interoperability between legacy, transitional, and NG911 networks, as well as progress towards achieving national NG911 interoperability. CSRIC VII collaborated with DOT's National 911 Program Office, DOC, industry, and trade associations, as well as state and local partners to develop this report.

LOOKING AHEAD TO 2020-2025:
Cybersecurity Recommendations for Federal Departments and Agencies

1. Emphasize cybersecurity awareness, cultivate cybersecurity information sharing, and improve information sharing governance bodies
2. Share guidance and best practices for implementing cybersecurity into public safety communications infrastructure
3. Implement additional cybersecurity training on how to protect public safety communications equipment and infrastructure

[20] FCC, CSRIC VII Report on the Current State of Interoperability in the Nation's 911 Systems. March 2020. https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-vii

V. Conclusion

In 2019, federal departments and agencies coordinated across all levels of government to provide public safety communications capabilities in support of emergency response operations. Using the 2019 NECP as a roadmap, federal stakeholders worked towards increasing interoperable communications capabilities, both within organizations and in partnership with SLTT governments. Federal partners demonstrated progress towards achieving NECP goals and identified barriers to increased interoperability, including:

- Strengthened governance structures, increasing interoperability coordination between components, and streamlined administration of communications programs
- Obtained additional resources to close specific communications gaps to plan for future interoperability projects and applied lessons learned to increase continuity of communications during emergency events
- Identified training and exercise needs, including standardized training, assessment, and testing criteria
- Continued to scope the use of NIMS for their unique missions and partnerships for sharing communications infrastructure
- Explored partnerships to increase emerging communications capabilities, such as NG911, and leveraged real-world events to demonstrate the positive impact of interoperability projects
- Identified cybersecurity gaps in communications systems, such as information sharing between partners and enhanced training requirements

Moving forward, the 2019 ASA findings will help to identify interagency priorities and develop future ECPC initiatives for improving interoperability and public safety communications. The ECPC recommends federal departments and agencies consider these findings in their strategic planning processes. Through this effort, departments and agencies may better coordinate interoperability decisions and investments, enhance interoperability during response operations, and strengthen the ability of partners at all levels of government to prepare for, respond to, and recover from natural disasters, acts of terrorism, and other emergency events.

VI. Appendices

Appendix A: Interview Participants

Department or Agency	Component
Department of Agriculture	Office of Homeland Security
	Service Management Division, Office of the Chief Information Office
Department of Commerce	Enterprise Strategy, First Responder Network Authority
	Office of Public Safety Communications, National Telecommunications and Information Administration
Department of Defense	Office of the Secretary of Defense
	United States Navy
	White House Military Office
	Defense Information Systems Agency
Department of Energy	Office of the Chief Information Officer
Department of Health and Human Services	Office of Emergency Management and Medical Operations
Department of Homeland Security	Cybersecurity and Infrastructure Security Agency
	Federal Emergency Management Agency
	Unites States Coast Guard
	United States Secret Service
Department of the Interior	Radio Program & Spectrum Management Division, Information Resources Directorate, National Park Service
	Office of the Chief Information Officer
	Bureau of Land Management
Department of Justice	Federal Bureau of Investigation
	FBI Operational Technology Division/Radio Coordination Unit
Department of Labor	Emergency Management Center

Department or Agency	Component
Department of State	Bureau of Information Resource Management
	Office of Emergency Management
Department of the Treasury	Internal Revenue Service Criminal Investigations
	Treasury Inspector General for Tax Administration
Department of Transportation	Office of Intelligence, Security, and Emergency Services
	Office of the Chief Information Officer
Federal Communications Commission	Operations and Emergency Management Division
	Policy and Licensing Division
	Public Safety Homeland Security Bureau
	Cybersecurity and Communications Reliability Division
General Services Administration	Office of Mission Assurance
	Office of Continuity of Operations

Appendix B: Abbreviations/Definitions

ASA	Annual Strategic Assessment
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
COML	Communications Unit Leader
COOP	Continuity of Operations Plan
COVID-19	Coronavirus Disease
CSRIC	Communications Security, Reliability, and Interoperability Council
DHS	Department of Homeland Security
DOC	Department of Commerce
DOD	Department of Defense
DOE	Department of Energy
DOI	Department of the Interior
DOJ	Department of Justice
DOL	Department of Labor
DOS	Department of State
DOT	Department of Transportation
EAS	Emergency Alert System
ECPC	Emergency Communications Preparedness Center
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FSLTT	Federal, State, Local, Tribal, and Territorial
GAO	Government Accountability Office
HHS	Department of Health and Human Services
JWPMO	Joint Wireless Program Management Office
LMR	Land Mobile Radio
MOU	Memoranda/Memorandum of Understanding

NCR	National Capital Region
NECP	National Emergency Communications Plan
NG911	Next Generation 911
NIMS	National Incident Management System
NIST	National Institute of Standards and Technology
NQS	National Qualification System
NS/EP	National Security/Emergency Preparedness
NSSE	National Special Security Event
OMB	Office of Management and Budget
OMD	Office of the Managing Director
PKEMRA	Post-Katrina Emergency Management Reform Act of 2006
POC	Point of Contact
PSAP	Public Safety Answering Point
R&D	Research and Development
SOC	Security Operations Center
Treasury	Department of the Treasury
USCG	United States Coast Guard
USDA	United States Department of Agriculture
USSS	United States Secret Service
WCB	Wireless Communications Board

Appendix C: ASA Interview Questions

Each department and agency interview was tailored to address the successes, challenges, and missions unique to the organization being interviewed based on responses to previous years' interview questions. The below questions represent the generic structure that guided each interview.

Federal Profile

1. Provide 2-3 minutes for participants to review their department/agency Federal Profile.
2. Have participants determine if their Federal Profile needs to be revised. If the Federal Profile needs to be revised have the group identify a champion to update the document following the workshop.
3. If the Federal Profile does not need to be updated, move forward with posting the current version to the Max.gov website (Max.gov can only be accessed by other federal employees. This is not a public facing website).

Coordinating Bodies

1. Last year, your department indicated it participates in the following <number of> coordinating bodies:
    a. <Reference coordinating bodies from previous year ASA summary>
2. Does your department still participate in these coordination groups? Did your department establish or join any new coordinating groups in 2019?
3. Did your department's participation in these coordinating groups influence the outcome of any internal or external emergency communications polices, practices, trainings, cybersecurity, 911, Broadband, or LMR policies, programs, or projects?
4. Did any of these coordinating bodies produce guides or best practices, such as white papers or other guidance documents in 2019, that you would be willing to share with us?

Governance and Leadership

1. Does your department/agency have a formal governance or decision-making body that coordinates interoperable communications policy across components?
    a. *If yes*, how has your department/agency's governance structure strengthened interoperable communications in the last year?
    b. *If no*, what are the barriers to creating a formal governance body for interoperable communications?
        i. How does your department/agency coordinate internal communications policy?
        ii. How does your department/agency coordinate communications decisions with any external partners (e.g., other federal organizations)?

2. How does your department/agency prioritize funding for communications needs (e.g., allocations for communications systems, areas of investment, systems to sustain)?
    a. How does your department/agency balance sustainment of existing communications systems/technologies with building new communications capabilities?
3. How does your department/agency incorporate input from internal stakeholders (e.g., end users, technical staff, and senior leadership)?
4. Does your department/agency's governance body incorporate external partners (e.g., other federal entities, state, local, tribal, or territorial stakeholders)?
5. How does your department/agency's governance or decision-making body coordination with other federal partners?
6. How does your department/agency's governance structure assess the impact of emerging technologies (e.g., Fifth Generation, Internet of Things devices)?
7. Is your department/agency actively planning to implement any emerging technologies?
    a. *If yes*, please describe which technologies, your governance body's approach, and any challenges/success outlined.
    b. *If no*, how does your governance body assess the impact of emerging communications technologies on your department/agency's mission?

Planning and Procedures

1. How often does your department/agency update interoperable communications plans?
2. In 2019, did your department/agency make any significant changes to communications strategic plans?
    a. *If yes*, what factors facilitated any change(s)?
    b. *If no*, how will your department/agency evaluate future strategic communications needs?
3. How does your department/agency determine strategic plans, goals, and milestones for communications systems?
4. How does your department/agency measure success towards achieving communications interoperability?
5. What major risks to communications capabilities did your department/agency prepare for in 2019 (e.g., weather hazards, technical limitation, etc.)?
6. How does your department/agency plan to mitigate the risk(s) outlined above?
7. In 2019, did your department/agency incorporate any new resiliency measures into communications systems?

Training, Exercises, and Evaluation

1. How does your department/agency determine the technical and operational skills required to fulfill your communications capabilities?
    a. How does your department/agency ensure communications staff meet technical and operational skill requirements?

2. In 2019, did your department/agency identify any technical or operational capability gaps as a result of training/exercise engagements?
    a. *If yes*, what actions did your department/agency take to close capability gap(s)?
    b. *If no*, how does your department/agency evaluate communications capabilities during training/exercises?
3. In 2019, did your department/agency participate in [example major federal exercises]?
    a. *If yes*, what communications successes or challenges did your department/agency identify by participating?
4. In 2019, did your department/agency field test any communications systems to ensure interoperability?
    a. *If yes,* how often did your organization test capabilities? How did your organization determine success indicators and evaluate outcomes?
    b. *If no*, how does your department/agency evaluate communications system interoperability outside of response operations?
5. In 2019, did your department/agency engage in communications training/exercises with other federal partners?
    a. *If yes*, how did your department or agency identify challenges, successes, and mitigation strategies (e.g., after-action reports)?
    b. *If no*, were there any factors that impacted training/exercise engagements with other federal partners?

Communications Coordination

1. In 2019, did your department/agency sponsor staff for communications specific-NIMS trainings?
    a. *If yes*, how has NIMS training impacted your department/agency's communications staff skills?
    b. *If no*, does your department/agency have plans to implement NIMS communications training requirements? What factors influence your department/agency's decision?
2. Does your department/agency use NIMS resource typing definitions for communications assists?
    a. *If yes*, how has NIMS resource typing impacted your department/agency's communications assets?
    b. *If no,* does your department/agency have plans to implement NIMS resource typing for communications assets? What factors influence your department/agency's decision?
3. In 2019, did your department/agency participate in any response operations with other federal, state, local, tribal, or territorial partners?
    a. *If yes*, did your department/agency identify any communications-related operational challenges (e.g., spectrum management, broadband capacity, incompatible equipment)?
    b. *If no*, how does your department/agency prepare communications assets for multi-agency/multi-jurisdictional response operations?

4. Does your department have any formal written agreements with FSLTT entities that define roles and responsibilities during response operations (e.g., MOU agreements, inter-agency agreements)?
    a. *If yes*, with whom do you have agreements? How did formal agreements with defined roles and responsibilities impact response operations?
    b. *If no*, has there been discussion within your organization to establish formal agreements? What factors prevent establishing formal agreements?
5. How does your department/agency evaluate and update operational communications protocols/procedures?
6. How does your department/agency evaluate new communications technologies to ensure interoperability with existing systems?
    a. In 2019, did your department/agency evaluate any shared communications technology with other federal partners? *If yes,* what successes or challenges did your department/agency identify?
7. In 2019, how did your department/agency ensure continuity of communications during response operations?
    a. Did your department or agency encounter any challenges maintaining reliable/interoperable communications? *If yes*, how did your department/agency close that capability gap?
8. In 2019, how did your department/agency incorporate communications interoperability and resiliency into continuity of operations planning/exercise?

Technology and Infrastructure

1. How does your department/agency evaluate new communications technologies to ensure interoperability with existing systems?
    a. In 2019, did your department/agency evaluate any shared communications technology with other federal partners? *If yes,* what successes or challenges did your department/agency identify?
    b. In 2019, did your department/agency use any commercial/off-the-shelf solutions to close a capability gap?
    c. *If yes,* what factors influenced your department/agency's decision to rely on a commercial/off-the-shelf solution?
2. In 2019, did your organization conduct any multi-organizations pilot programs?
3. How do you share information about research and development (R&D) projects and communications technology investments?
4. How does your department/agency evaluate current and future communications needs (e.g., technologies, assets, capacity, etc.)?
5. In 2019, did your department/agency share or plan to share any communications systems or infrastructure with other federal partners?
    a. *If yes*, what influenced your organization's decision to leverage shared systems/infrastructure? Does your department/agency plan to expand shared communications/infrastructure?

    b. *If no*, were there any factors that prevented your organization from sharing communications/infrastructure with other federal partners?

6. How does your department/agency incorporate communications standards (e.g., Project 25)?
7. Does your department/agency operate any public safety answering points (i.e., emergency communications centers, 911 dispatch offices, public safety communications points)?
    a. *If yes*, has your department/agency begun implementing Next Generation 911 standards?
    b. *If yes*, how does your organization assess NG911 maturity across your 911 infrastructure?
    c. *If no*, are there any factors that inhibit the transition to NG911 standards?
    d. *If no,* how does your department/agency assess and respond to emergency calls on lands/facilities administered by your organization?

Cybersecurity

1. In 2019, did your department/agency share cybersecurity threat information with other federal, state, local, tribal, or territorial partners?
    a. *If yes*, how does your organization share information? Did information sharing help prepare your department/agency against cyber threats?
    b. *If no*, does your organization plan to participate in any cybersecurity information sharing mechanisms (e.g., DHS National Cybersecurity and Communications Integration Center)
2. In 2019, how did your department/agency identify communications equipment or systems cybersecurity vulnerabilities?
    a. *If yes*, how did your organization mitigate communications equipment or systems vulnerabilities?
    b. *If no*, how does your department/organization evaluate existing/future communications systems for cybersecurity vulnerabilities?
3. Is your department/agency currently employing the National Institute of Standards and Technology (NIST) Cybersecurity Framework or a similar standard?
    a. *If yes*, how did the adoption of cybersecurity standards impact communications interoperability? Did your organization identify any challenges (e.g., training gaps)?
    b. *If no,* does your organization plan to adopt a NIST Cybersecurity Framework-like standard? What factors inhibit adoption?
4. Does your department/agency regularly conduct cybersecurity training/tests with end-users (e.g., phishing simulations)?

Appendix D: ASA Alignment to 2016 Government Accountability Office Findings

In 2016, the GAO reviewed the implementation of the Post-Katrina Emergency Management Reform Act of 2006 (PKEMRA), to include (1) federal efforts to implement PKEMRA emergency communications provisions related to planning and federal coordination, and (2) how states' emergency communications planning has changed since the passing of PKEMRA.

The GAO found the ECPC's collaborative efforts improved coordination and information sharing among federal emergency communications programs. However, the GAO identified an area for improvement in that the ECPC does not actively track its member departments' and agencies' implementation of ECPC recommendations. The GAO found that while the ECPC puts forth recommendations to improve emergency communications, these are implemented at the discretion of the ECPC's member departments and agencies. As a result, the GAO recommended the ECPC should institute a mechanism to track ECPC members' implementation of recommendations.

Through tailored interviews, the ASA seeks to track the status of ECPC recommendations amongst ECPC's member departments and agencies. ASA interview questions are grounded in ECPC recommendations for its members and include NECP goals and objectives (e.g., establishing a department-wide interoperability coordinator). As stated in the GAO report, the ASA provides information on federal coordination efforts, defines opportunities for improving federal emergency communications, and reports on the progress of implementing the ECPC working groups' and focus groups' recommendations.

The ECPC concurred with the GAO's finding that the ECPC needs a formal tracking mechanism for implementation of ECPC recommendations. The ECPC Steering Committee is currently considering ways to track ECPC member departments' and agencies' implementation of ECPC recommendations. This tracking mechanism may be addressed in future iterations of the ASA.