



Emergency Communications Preparedness Center: Annual Strategic Assessment

Calendar Year 2023 Report to Congress

December 2024



Homeland
Security

*Cybersecurity and
Infrastructure Security
Agency (CISA)*

Message from the Director

January 16, 2025

On behalf of the Cybersecurity and Infrastructure Security Agency (CISA) Emergency Communications Preparedness Center (ECPC), I am pleased to submit to Congress the 2023 ECPC Annual Strategic Assessment (ASA). Congress authorized the establishment of the ECPC in 2009, which serves as the federal focal point for operable and interoperable communications coordination. The ECPC coordinates the roles and activities of agencies across the federal government to improve interoperable public safety and emergency response communications. It consists of 14 federal departments and agencies representing the federal government's role in improving coordination of emergency communications efforts, including information sharing, planning, regulation, policy, operations, grants, and technical assistance. The ECPC is administered by the U.S. Department of Homeland Security's CISA.



This document was compiled pursuant to 6 United States Code (U.S.C.) § 576. The ASA assesses federal coordination efforts toward improving the continuity and interoperability of communications in key areas found in the goals and objectives of the 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.

Throughout 2023, agencies continued to face ongoing challenges shaped by constraints on financial and physical infrastructure resources and continued to collaborate on emergency communications despite the lack of formal strategic emergency communications planning. These challenges, and how federal agencies continued to respond to them, determined the ability of federal agencies to coordinate resources and effectively maintain steady-state and emergency response operations throughout the year.

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

The Honorable Mark E. Green
Chairman, House Committee on Homeland Security

The Honorable Bennie G. Thompson
Ranking Member, House Committee on Homeland Security

The Honorable Brett Guthrie
Chairman, House Committee on Energy and Commerce

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

The Honorable Rand Paul
Chairman, Senate Committee on Homeland Security and Governmental Affairs

The Honorable Gary C. Peters
Ranking Member, Senate Committee on Homeland Security and Governmental Affairs

The Honorable Ted Cruz
Chair, Senate Committee on Commerce, Science, and Transportation

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

Sincerely,

A handwritten signature in black ink, appearing to read "Jen Easterly". The signature is fluid and cursive, with a large initial "J" and a long, sweeping tail.

Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency

Executive Summary

The Emergency Communications Preparedness Center (ECPC) was established by 6 United States Code (U.S.C.) § 576 to improve interoperable communications coordination among federal agencies. The ECPC is comprised of 14 federal departments and agencies who meet regularly to address gaps in federal emergency responders' abilities to communicate across jurisdictions and functions. Pursuant to authorizing statutes, the ECPC developed the Annual Strategic Assessment (ASA) to evaluate federal interoperability with appropriate partner agencies and the impact of coordination on continuity of communications and interoperability during day-to-day operations and during out-of-the-ordinary emergencies or disasters.

Reliable and interoperable communications capabilities are critical to enabling federal, state, local, tribal, and territorial (FSLTT) public safety and national security and emergency preparedness (NSEP) 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 across all levels of government.

The ECPC ASA examines progress on federal coordination efforts defined by the six goals of the National Emergency Communications Plan (NECP)¹: (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 toward accomplishing each goal of the NECP.

The ECPC ASA documents communications efforts during coordinated responses to large-scale disasters, planned events, routine public safety operations, and exercises that tested the interoperability of federal agencies. The ECPC ASA analyzes the successes, challenges, and lessons learned from these efforts. This report reflects current federal priorities for improving emergency communications, identifies progress made by the federal government against opportunities identified in past years, and outlines opportunities for further federal coordination in the years ahead.

In 2023, the ECPC found that federal agencies continued to prioritize cybersecurity hygiene and leverage strong interagency relationships to ensure the operability and interoperability of emergency communications. Federal agencies approached interoperable communications from multiple perspectives, including:

- Continuing involvement in inter-governmental governance bodies, and building strong relationships with interagency partners and expanded stakeholders, beyond those strictly aligned within public safety or emergency management domains

¹ CISA, National Emergency Communications Plan. [cisa.gov/necp](https://www.cisa.gov/necp)

- Addressing emergency communications gaps in strategic plans, incorporating robust risk-management strategies, and continuing pre-incident communications planning
- Leveraging the planning for and execution of support to National Special Security Events (NSSEs), Special Event Assessment Rating (SEAR) events, National Level Exercises, and shared communication partnerships to train, test, and improve communication systems and collaborate with one another
- Expanding sharing agreements between FSLTT partners and developing resilience and continuity of communication plans throughout operations
- Investing in fifth generation (5G) wireless communications technology deployment and participating in forums on advanced technologies
- Sharing cybersecurity data, resolving cyberattacks quickly, and utilizing Cybersecurity and Infrastructure Security Agency (CISA) as the foremost authority for cybersecurity guidance

More information on these key findings can be found in **Section III**.

2023 Annual Strategic Assessment

Contents

| | |
|--|------------|
| Message from the Director | i |
| Executive Summary | iii |
| 2023 Annual Strategic Assessment | v |
| I. Statutory Language | 1 |
| II. Scope and Methodology | 2 |
| Scope and Analytical Framework | 2 |
| Data Collection Approach | 2 |
| Data Analysis Approach | 3 |
| III. Summary of 2023 ASA Findings and Recommendations | 4 |
| IV. Analysis | 8 |
| Governance and Leadership | 13 |
| Challenges and Priorities | 14 |
| Successes | 15 |
| Planning and Procedures | 19 |
| Challenges and Priorities | 19 |
| Successes | 21 |
| Training, Exercises, and Evaluation | 21 |
| Challenges and Priorities | 21 |
| Successes | 23 |
| Communications Coordination | 26 |
| Challenges and Priorities | 26 |
| Successes | 27 |
| Technology and Infrastructure | 29 |
| Challenges and Priorities | 30 |
| Successes | 32 |
| Cybersecurity | 34 |
| Challenges and Priorities | 34 |
| Successes | 36 |
| IV. Conclusion | 39 |
| V. Appendices | 40 |

I. Statutory Language

6 United States Code (U.S.C.) § 576² sets forward the following provisions:

(c) FUNCTIONS: The Center shall—

- (1) Serve as the focal point for interagency efforts and as a clearinghouse with the 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 2023 ECPC Annual Strategic Assessment (ASA) meets the requirements outlined in 6 U.S.C. § 576. It provides information on federal coordination efforts and documents their impact on communications interoperability and the ability of public safety response providers to continue to communicate in the event of disasters, acts of terrorism, other human-caused disasters, and planned events. The ECPC leveraged principles from the National Emergency Communications Plan (NECP) and the SAFECOM Interoperability Continuum³ to develop the 2023 ECPC ASA.

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

³ CISA, Interoperability Continuum: A Tool for Improving Emergency Response Communications and Interoperability, 2021. <https://www.cisa.gov/safecom/resources>.

II. Scope and Methodology

As the administrator of the Emergency Communications Preparedness Center (ECPC), the Cybersecurity and Infrastructure Security Agency (CISA) developed the 2023 ECPC Annual Strategic Assessment (ASA) with input and coordination from federal agencies.⁴ The following section describes the ASA scope, data collection approach, analysis process, and procedures for review of department and agency-specific emergency communications profiles. The ECPC ASA evaluates improvements in federal emergency communications and federal coordination, highlighting capabilities that support emergency preparedness and response activities. Through the compilation of best practices and lessons learned, this assessment is a resource to enable federal agencies to enhance communications continuity and interoperability.

Scope and Analytical Framework

The ECPC ASA details federal emergency communications activities from the 2023 calendar year, including planned events, federal programs, exercises, investments, and responses to disasters. The ASA is intended to serve as a representative summary, rather than a comprehensive accounting of all federal emergency communications activities. The 2023 ECPC ASA findings align to the National Emergency Communications Plan (NECP) goals and the SAFECOM Interoperability Continuum,⁵ providing a common framework for identifying challenges, trends, and lessons learned.

Data Collection Approach

In 2023, the federal government continues to operate in a hybrid work environment following the Coronavirus Disease (COVID-19) pandemic. In past years, CISA gathered data through in-person and virtual interviews with each department and agency. A change in this data collection approach came in 2019, when CISA hosted the first-ever in-person ASA Interagency Summit. During this 2019 Summit, federal agencies shared their individual ASA-related data, while collaborating with other federal stakeholders to identify trends and other common challenges and solutions. Recognizing the benefits of these past data collection methods, CISA combined data collection methods in 2023, conducting eleven two-hour virtual interviews with individual ECPC member agencies and hosting a virtual and in-person collaborative interagency two-day Summit in March of 2024.

For each departmental interview, CISA tailored approximately 90 interview questions which were aligned to the NECP goals. The intent of the interviews was to gather detailed information on emergency communications challenges, opportunities, and successes at the department and

⁴ 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).

⁵ CISA, SAFECOM Interoperability Continuum, June 2021. https://www.cisa.gov/sites/default/files/2022-12/21_0615_cisa_safecom_interoperability_continuum_brochure_final.pdf.

agency level. The interview questions were based on open-source research and responses from previous ASA interviews.

Data Analysis Approach

In support of the 2023 Emergency Communications Preparedness Center (ECPC) Annual Strategic Assessment (ASA), the Cybersecurity and Infrastructure Security Agency (CISA) gathered extensive quantitative and qualitative notes from federal agency interviews, ASA Summit data gathering efforts, and follow-up outreach and interviews. CISA utilized results from the interviews and ASA Summit to review federal coordination and success towards achieving the National Emergency Communications Plan (NECP) goals and recognize potential areas of opportunities for improvement.

III. Summary of 2023 ASA Findings and Recommendations

The following tables provide a summary of the 2023 ECPC ASA key findings and recommendations, structured by the NECP goals: (1) Governance and Leadership; (2) Planning and Procedures; (3) Training, Exercises, and Evaluation; (4) Communications Coordination; (5) Technology and Infrastructure; and (6) Cybersecurity.

Table 1: 2023 ECPC ASA Key Findings

| SECTION | KEY FINDING |
|---|---|
| <p>Governance and Leadership</p> | <ol style="list-style-type: none"> 1. Federal departments and agencies were more actively engaged in inter-governmental governance bodies (e.g., Emergency Communications Preparedness Center [ECPC], SAFECOM, National Council of Statewide Interoperability Coordinators [NCSWIC], Federal Partnership for Interoperable Communications [FPIC], Federal Executive Boards, Urban Area Security Initiatives) 2. Federal departments and agencies continued to maintain strong interagency governance relationships ensuring effective coordination and decision-making 3. Federal Civilian Executive Branch (FCEB) agencies demonstrated consistent inclusion of expanded stakeholders (e.g., information technology [IT] staff and private sector) in communications governance processes |
| <p>Planning and Procedures</p> | <ol style="list-style-type: none"> 1. Although many FCEB agencies did not address emergency communications within strategic plans, those which did reported progress toward closing associated gaps 2. Federal agencies incorporated robust risk management strategies within their continuity and recovery plans 3. FCEB agencies reported continued collaborative pre-incident communications planning, ensuring interoperability for incidents and special events |
| <p>Training, Exercises, and Evaluation</p> | <ol style="list-style-type: none"> 1. National Security Special Events (NSSE) were successful opportunities for federal departments and agencies to train, exercise, evaluate, and collaborate on emergency communications priorities 2. Exercises continue to test federal readiness and continuity of communications systems and functions 3. Emergency Alert System (EAS) Nationwide Tests continue to be utilized for public notification and EAS owners/operators continue to seek opportunities for improvement of notifications |

| SECTION | KEY FINDING |
|--|---|
| <p align="center">Communications Coordination</p> | <ol style="list-style-type: none"> 1. Some federal departments and agencies eliminated their National Incident Management System (NIMS) trainings due to funding constraints 2. Federal departments and agencies explored and implemented shared communications infrastructure where possible, but there are more opportunities to do this 3. Federal departments and agencies continue to establish strong interoperability agreements with other federal, state, local, tribal, and territorial (FSLTT) partners 4. Federal departments and agencies continued to implement resiliency and continuity of communications plans throughout their operations |
| <p align="center">Technology and Infrastructure</p> | <ol style="list-style-type: none"> 1. Transition to Next Generation 911 (NG911) across the federal landscape is inconsistent or not being pursued 2. There is continued federal reliance on commercial-off-the-shelf (COTS) solutions 3. Federal departments and agencies continue to prepare for significant investments in fifth generation (5G) capabilities 4. Departments and agencies are working cooperatively to ensure communications success using research and development (R&D) efforts |
| <p align="center">Cybersecurity</p> | <ol style="list-style-type: none"> 1. Few agencies reported implementation of the National Institute of Science and Technology (NIST) Cybersecurity Framework, and among those who have, they continue to find gaps in implementation 2. Zero-Trust Architecture (ZTA) and Multi-factor Authentication (MFA) implementation remain priorities for federal entities, but the level of completion varies across the federal landscape 3. Departments and agencies successfully and continuously share cybersecurity-related data with FSLTT partners 4. Cyberattacks were resolved quickly and had minimal impact on federal emergency communications operations in 2023 5. Agencies continue to look to the Cybersecurity and Infrastructure Security Agency (CISA) for guidance on cyber hygiene and cybersecurity information sharing |

Table 2: 2023 ECPC ASA Recommendations

| SECTION | RECOMMENDATION |
|---|--|
| <p>Governance and Leadership</p> | <p>1. Federal agencies should continue striving to implement a dedicated Federal Interoperability Coordinator (FIC) position to serve as a lead coordinator for emergency communications planning and response, thereby improving decision-making, relationship-building, and the agency’s ability to respond decisively when emergency communications interoperability incidents arise</p> |
| <p>Planning and Procedures</p> | <p>1. Federal agencies should include details about mandates, timelines, and inspections as part of their emergency communications standard procedures to ensure emergency communications strategic plans are being updated, exercised, and implemented regularly and effectively</p> <p>2. Federal departments and agencies should carefully integrate emergency communications priorities into their strategic plans to ensure adequate priority, attention, and resources can be dedicated to the domain</p> |
| <p>Training, Exercises, and Evaluation</p> | <p>1. Federal departments and agencies should strive to keep detailed records of communications-focused exercises and lessons learned to ensure that challenges and gaps are addressed</p> <p>2. Federal agencies should share resources and open trainings to other federal and state, local, tribal, and territorial (SLTT) partners to strengthen their pre-event relationships and improve communications during unplanned and emergency events</p> |
| <p>Communications Coordination</p> | <p>1. Federal entities should continue to encourage the use of National Incident Management System (NIMS)-compliant assets across the federal interagency landscape</p> <p>2. Federal departments and agencies should continue to discover and pursue collaborative partnerships for shared emergency communications services that address roles, responsibilities, liabilities, spectrum, infrastructure, data interoperability, cybersecurity, and data sharing needs</p> |
| <p>Technology and Infrastructure</p> | <p>1. Federal departments and agencies should evaluate the risks in emergency communications supply chains and build plans to ensure that federal agencies equipment lifecycles can be maintained</p> <p>2. Federal entities should establish dedicated lines of funding to support the maintenance and modernizations of federal emergency communications systems in accordance with their primary, alternate, contingency, and emergency (PACE) plans for tactical, operational, and strategic emergency communications operations</p> |

| SECTION | RECOMMENDATION |
|---|---|
| <p style="text-align: center;">Cybersecurity</p> | <ol style="list-style-type: none"> 1. Federal departments and agencies should seek tailored cybersecurity assistance from federal partners to ensure they receive specific and actionable guidance regarding industry standards and executive direction to keep their systems secure, operable, and interoperable 2. Federal departments and agencies should continue to share cybersecurity threat information with other FSLTT partners to continue building resilient relationships and identify potential threats within the federal cybersecurity sphere of responsibility 3. Federal departments and agencies should remain diligent in working with vendors to ensure cyber threats are identified and mitigated prior to serious cybersecurity breaches 4. Federal departments and agencies should continue to follow cybersecurity guidance as it relates to ZTA and MFA |

IV. Analysis

The 2023 Emergency Communications Preparedness Center (ECPC) Annual Strategic Assessment (ASA) examined major events impacting continuity of communications and interoperability in alignment with the six National Emergency

Emergency Communications Defined

The means and methods for exchanging information necessary for successful incident management⁶

Communications Plan (NECP) strategic goals, including: **Governance and Leadership, Planning and Procedures, Training, Exercises and Evaluation, Communications Coordination, Technology and Infrastructure, and Cybersecurity**. The following pages contain a summary of findings and spotlight successes and challenges in federal emergency communications coordination in 2023.

Governance and Leadership

ASA Definition: Coordination and decision-making processes that guide interoperable communications priorities and policy⁷

Corresponding NECP Goal 1: 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

Public safety agencies require strong and stable governance structures to support all aspects of emergency communications, such as resolving interoperability challenges, strategic planning, training and exercise strategy, and to benefit from policy improvement. In 2023, federal agencies identified several gaps; specifically, a lack of resources to support upgrades and updates to critical systems, the absence of Federal Interoperability Coordinators (FICs), and a governance void over nationwide 911 efforts. Despite these challenges, federal agencies continued to show strong participation in inter-governmental governance bodies, maintained robust interagency governance relationships, and continued collaborating with interagency partners and expanded stakeholders, beyond those strictly aligned within public safety or emergency management domains.

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

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

Challenges and Priorities

Lack of resources limit upgrades, updates, and maintenance of critical systems

Federal agencies engage in a great deal of coordination, planning, and training to sustain interoperable communications. Underpinning all these operations is the physical equipment itself that facilitates communication. In 2023, Federal Civilian Executive Branch (FCEB) agencies reported that budget constraints continue to cause concern for federal departments and agencies as these constraints directly impacted their ability to implement upgrades, updates, and maintenance of critical systems.

For example, the United States Coast Guard (USCG) reported that the funding needed to physically enhance equipment for interoperability is limited, noting that communication assets require updates, replacements, and continuous funds for sustainment. The USCG also shared that the previously reported challenge of the lack of a standard push-to-talk (PTT) cellular application is still a gap. They noted that while they occasionally use applications to collaborate with other agencies, the USCG does not have its own solution. U.S. Customs and Border Protection (CBP) reported that funding is limited and may require trade-off decisions in the year of execution. The United States Secret Service (USSS) reported they are currently operating radio systems equipment approaching 30 years of age across the nation due to reductions in enacted funding for reprioritization. The Department of Labor (DOL) attempts to maintain previously funded items in the budget, but expansion beyond budgeted resources is not currently possible.

To ensure federal interoperability, federal agencies should establish dedicated lines of funding, similar to the Department of Defense's (DoD) Base Emergency Communications System (BECS) program, to support the maintenance and modernization of emergency communications equipment and technology. The BECS program serves as the single integrated acquisitions program for the design, procurement, fielding, training, and lifecycle management of emergency management and critical communications capabilities.

Continued lack of the establishment of FICs

Interoperable communications do not occur by accident. They are the result of intentional planning and implementation by agencies whose missions require effective, uninterrupted, and secure emergency communications. To guarantee interoperability is maintained throughout agencies and within the federal community, the Cybersecurity and Infrastructure Security Agency (CISA) and the NECP have recommended the implementation of FICs within each ECPC member agency. FICs are intended to serve as an agency's primary point of contact to aid and facilitate the coordination and decision-making process for emergency communications.

In 2023, FCEB agencies did not report any planning efforts dedicated to implementing a department-wide FIC. To contend with the absence of a FIC, some federal agencies and their components utilize alternative mechanisms to fill this need. For example, the Department of the Interior (DOI) uses the Field Communications Improvement Executive Leadership Team as a mechanism for coordinating disparate preparedness response and emergency services within the department, and to make governance decisions related to communications interoperability. The participants meet quarterly and include the Chief Information Officer (CIO) and senior officials

from across the bureaus. Similarly, the Department of State (DOS) designates its Major Events Coordinator task force to address internal, external, and international emergency communications challenges as well as their Crisis Management Center to facilitate multi-agency response operations.

Identifying a central coordinator for incident response can improve decision-making, partnerships, consistency, and adaptability of federal communications programs and improve an agency's overall ability to respond in a coordinated manner throughout all levels of government, jurisdictions, disciplines, and organizations. Interoperable, effective, uninterrupted, and secure communications interoperability is mission essential for federal departments and agencies, and as such requires a designated resource, such as a FIC. Federal agencies should continue to explore ways to implement a dedicated FIC position to ensure progress toward nationwide interoperability.

Governance void over national 911 efforts

In 2023, FCEB agencies reported concerns about the lack of nationwide governance over 911 authority and the risks that this poses to nationwide interoperability. Without a singular entity responsible for managing and leading these efforts, guidance around 911 has been inconsistent and has failed to address critical issues. This has created significant challenges for states seeking to interoperate and interconnect 911 systems with one another, as well as federal agencies, as legislation and requirements vary widely between jurisdictions.

In 2023, the DoD reported a lack of governance dedicated to facilitating federal 911 interoperability. For instance, after attending a National Emergency Number Association conference, the DoD learned that many states are unwilling to extend their 911 services beyond their strict borders due to their state's legislation. As a result, federal entities have difficulty interconnecting and interoperating with state agencies or state 911 offices. The DoD shared their view that without governance and/or a singular governing body that holds federal authority over 911 efforts, this challenge will continue to hinder nationwide 911 interoperability and impact response to residents. Therefore, the DoD recognized the need for governance to achieve an interoperable national 911 solution.

Additionally, the expiration of the 911 Implementation and Coordination Office's authority on September 30, 2022, is related to this situation. This expiration narrowed NHTSA's focus to exclusively highway safety and other Department of Transportation (DOT) initiatives, halting 911 grant efforts as well.

The Federal Communications Commission (FCC) has a role in NG911 implementation and has provided support for implementation efforts by state, local agencies, and 911 call centers through developing regulations on service providers (e.g. wireless and wireline). With the transition to NG911, state and local 911 authorities are replacing legacy circuit-switched 911 networks with Internet Protocol (IP)-based networks and applications that will support new 911 capabilities, including text, video, and data, as well as improved interoperability and system resilience. In June 2023, the FCC proposed rules to facilitate the transition to NG911 for various service providers. The proposed rules would require service providers to deliver 911 calls, including associated location information, in an IP-based format to designated NG911 delivery points when certain conditions are met. The proposed rule would also address telecommunications

providers' cost responsibility for transmitting 911 traffic in the required IP-based format and transmitting 911 traffic to the designated NG911 delivery points. In July 2024, after notice and comment, the Commission adopted final rules to facilitate the transition to NG911.

Successes

Strong involvement in external governance bodies

In 2023, FCEB agencies reported a high level of participation in external governance bodies such as SAFECOM, National Council of Statewide Interoperability Coordinators (NCSWIC), Federal Partnership for Interoperable Communications (FPIC), and ECPC. Agencies reported that engagement in external governance bodies has benefited their information sharing and coordination efforts which are critical to sustaining interoperability. Some agencies also reported maintaining involvement in such bodies to improve relationships and serve as a dutiful partner.

The Department of Treasury's (TREAS) Treasury Inspector General for Tax Administration (TIGTA) reported that its participation in the SAFECOM, FPIC, and National Telecommunications and Information Administration (NTIA) Spectrum groups has been helpful for TIGTA. However, TIGTA shared its desire for the reinstatement of the ECPC Interoperability Working Group, stating that it was valuable to provide a field-level perspective on how personnel are solving interoperability problems. FCC reported its Public Safety and Homeland Security Bureau (PSHSB) staff participate in SAFECOM, NCSWIC, CISA's Southwest Border Communications Working Group, and ECPC's Federal 911 Working Group, which has helped them better understand regulatory and interoperability activities. The Department of Justice (DOJ) reported participation in the ECPC Steering Committee, Advanced Technologies Working Group, and Federal Resource Sharing Working Group. DOJ shared that they participate primarily to continue serving as a reliable partner, but that these meetings are useful for coordination of efforts. NTIA, as the spectrum manager for the federal agencies, reports participation in the FPIC, a coordination and advisory body to address technical and operational wireless issues relative to interoperability within the public safety emergency communications community.

The DoD reported its participation in the newly formed Public Safety Communications Senior Steering Group, which provides coordination across the Office of the Secretary of Defense and gives them representation in a new forum that did not previously exist. This group involves all DoD stakeholders in an effort to help with policies and procedures. The USSS noted participation in the Metro Washington Council of Governments (MWCOC-DC) and the Department of Homeland Security (DHS) Joint Wireless Program Management Office (JWPMO) has improved its technical information sharing, ability to leverage lessons learned and input to the vendor community. Finally, the United States Department of Agriculture (USDA) participated in an Information Technology (IT) Modernization Working Group to ensure the emergency communications needs of the USDA and other federal departments and agencies are being met. The USDA also noted its recent involvement with the FPIC, which has provided the department with a great level of information-sharing opportunities. To better support and enhance interagency governance, federal agencies should continue to engage with the ECPC and other external governance bodies to highlight shared mission challenges and identify solutions.

 *Agencies maintain strong interagency governance relationships*

In 2023, FCEB agencies indicated sustained strength of interagency relationships. A key element of any governance structure is to cultivate robust relationships through collaboration and partnership. These relationships help to ensure effective coordination and decision-making for federal emergency communications interoperability.

Throughout the year, the FCC’s PSHSB Policy and Licensing Division engaged in intra- and interagency coordination on spectrum management policies, in addition to cross-border spectrum and frequency use agreements with Canada and Mexico. The FCC also recently adopted rules allowing participating agencies to share Network Outage Reporting System⁸ and Disaster Information Reporting System⁹ information with first responders, emergency communications centers (ECCs), and other local government agencies that play a vital public safety role during crises with “need to know.” These rules have streamlined information sharing with FCC partners and enhanced the Commission’s ability to allocate resources effectively.

DOJ, USCG, and U.S. Immigration and Customs Enforcement (ICE) all described their relationships with other federal partners as outstanding, which greatly enhanced their ability to promote interoperability. The DOJ specifically noted it extends invitations to other departments and agencies to participate in their training opportunities, including state and local task force officers, where officers are trained similarly to federal agents. Several agencies including FCC, DOC, DOT, and USDA also noted having a high degree of confidence in their partners. TIGTA shared it has never experienced any issues with a federal partner or been hesitant to share their resources, and ICE reported it has not experienced challenges at any level with another federal agency.

The USSS and USDA both reported maintaining strong relationships founded on technical solutioning. The USSS shared that it has wide-ranging relationships, and the communications technical community is robust in supporting one another across multiple missions. Similarly, USDA’s Office of Homeland Security (OHS) reported they participate in the Continuity of Communications Management Group, meeting regularly to discuss challenges and partner on solutions.

Additionally, CISA has also maintained a strong and collaborative relationship within DHS for knowledge sharing, strategic guidance, and participation in tabletop exercises with interagency partners as a means of ensuring and realizing considerations and threats to cybersecurity, communication infrastructure, and operational continuity throughout all of DHS operations. For example, CISA is a member and active participant in the DHS Office of Chief Readiness Support Officer (OCRSO), Critical Infrastructure Security and Resilience (CISR) working group. The OCRSO leads the resilience framework effort for the Department in collaboration with FEMA’s Office of National Continuity Programs (ONCP). The CISR working group includes representatives from all DHS Components in areas of continuity, facilities, information

⁸ FCC, Network Outage Reporting System (NORS), November 2023. <https://www.fcc.gov/network-outage-reporting-system-nors>.

⁹ FCC, Disaster Information Reporting System (DIRS), April 2024. <https://www.fcc.gov/general/disaster-information-reporting-system-dirs-0>.

communications technology (ICT), and transportation. Agencies should continue prioritizing activities which can support interagency relationship building. Strong partnerships and communication channels are essential for the coordination required to maintain federal emergency communications interoperability.

 *Continued incorporation of expanded stakeholders, beyond those strictly aligned within public safety or emergency management domains*

In 2023, FCEB agencies demonstrated frequent inclusion of expanded stakeholders, such as IT staff, private companies, and cybersecurity subject matter experts in communications, governance, and decision-making processes. This involvement helped improve policymaking and decreased the knowledge gap with Congressional representatives.

The DoD reported incorporating companies which manage commercial-off-the-shelf (COTS) capabilities between contractors and government entities, noting the importance of these capabilities with Congressional support. The FCC reported their non-federal state, local, tribal, and territorial (SLTT) partners provided input on public safety spectrum initiatives, ensuring that a federal perspective is not the only source of input during decision-making. The FCC also noted, with respect to cybersecurity, collaboration with federal partners is critical to ensure a harmonized, whole-of-government approach to policymaking, while acknowledging each partner's statutory authorities and scope of work.

The USDA reported a unique forum in its Integrated Advisory Board (IAB), which constitutes the collaboration of the Enterprise Architecture Committee, Portfolio and Investment Management Council, Enterprise Security Governance Council, and the 9 Critical Partners Advisory Group. Operating as a pivotal element within the Integrated IT Governance Framework, the IAB plays a crucial role in upholding accountability and ensuring the success of IT governance objectives. The primary purpose of the IAB is to establish a forum for technology leadership, assuring that all decisions about major IT investments align with the goals, strategies, objectives, and mission needs at the department, agency, and staff office levels. The IAB also functions in an advisory capacity, possessing the authority to submit technical recommendations for IT investments to the Enterprise Board. Additionally, the IAB is mandated to offer counsel and recommendations to the USDA CIO, who then provides recommendations to the Deputy Secretary.

DHS components also noted consistent collaboration with non-traditional stakeholders in 2023. USCG and Federal Protective Service (FPS) both reported leveraging an Integrated Product Team to bring together technical and user representatives. Meanwhile, the USSS indicated internal groups are incorporated for IT and cyber support, external partner agencies are leveraged for best practices and information sharing, and vendors are engaged for market availability and direct support efforts.

Agencies should continue to engage non-traditional stakeholders regularly as they make decisions about IT and commercial products as they can provide valuable insight. Agencies engaging non-traditional stakeholders note improved outcomes because of this collaboration.

LOOKING AHEAD:
Governance and Leadership Recommendation for
Federal Departments and Agencies



1. Federal agencies should continue striving to implement a dedicated FIC position to serve as a lead coordinator for emergency communications planning and response, thereby improving decision-making, relationship-building, and the agency's ability to respond decisively when emergency communications interoperability incidents arise

Planning and Procedures

ASA Definition: 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 technologies¹⁰

Corresponding NECP Goal 2: 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

Emergency communications planning and procedures specify daily operational processes which guide the deployment of resources and technologies, as well as strategic and multi-year plans which direct the continuity and resilience goals of each department and agency. In recent years, these plans have been integral to the flexibility and sustainment of federal emergency communications. In 2023, federal agencies identified several gaps; specifically, constraints hindering lifecycle planning, failure to address emergency communications within strategic plans, and failure to update those plans regularly. Despite these challenges, federal agencies made progress toward closing emergency communications gaps recognized within strategic plans, maintained robust risk management strategies in continuity and recovery plans, and continued collaborative pre-incident communications planning.

Challenges and Priorities



Constraints continue to hinder lifecycle planning

Lifecycle planning requires public safety agencies to evaluate risks, gaps, and barriers on the horizon to adjust plans and strategies in response to evolving threats and technologies. Lifecycle planning also aids federal agencies in long-term investment planning for interoperability solutions and maintenance costs. In 2023, FCEB agencies struggled to adequately address lifecycle planning to maintain communications assets. Time, available workforce, and most commonly, budget, were noted as barriers preventing agencies from conducting lifecycle planning.

¹⁰ CISA, National Emergency Communications Plan, 2019. <https://www.cisa.gov/publication/national-emergency-communications-plan>.

The USSS, DOJ, and USDA each reported a lack of funding and budget cycles have made it difficult to execute lifecycle planning. CBP noted a lack of time to conduct thorough analyses between submission deadlines acts as a primary barrier for the component. Finally, USCG reported its Communications Program staff do not have any professional cost estimators; therefore, estimations are typically a best guess from the project managers or engineers, who have varying levels of knowledge and experience with cost estimating. This has made accurate cost estimating a consistent barrier in lifecycle planning within USCG.

To mitigate challenges with lifecycle planning, federal agencies should reference resources such as the *Emergency Communications System Lifecycle Planning Guide*¹¹, which provides guidance on public safety communications system lifecycle planning. The document contains best practices for funding, planning, procuring, implementing, supporting, and maintaining public safety communications systems, and eventually replacing or disposing of outdated system components.

Strategic plans scarcely address emergency communications

In 2023, the ECPC found that FCEB agencies are infrequently addressing emergency communications goals, strategies, and timelines within their strategic plans. When emergency communications are not acknowledged within an agency's strategic plan, it can ultimately prove difficult to address needs or allocate resources to the field. Emergency communications should be included and prioritized as part of agencies' strategic plans as opposed to an afterthought.

Within DHS, the Transportation Security Administration (TSA), ICE Tactical Communications (TACCOM), and CBP, each noted that their strategic plans do not cover goals, strategies, or timelines related to emergency communications. The General Services Administration (GSA) also reported emergency communications are not addressed in its strategic plan, though many of these items are addressed in the GSA National Continuity Plan. TIGTA noted a lack of emergency communications acknowledgment within their strategic plan is one of their weaknesses, but they continue to make progress by addressing emergency communications within ancillary plans. For example, emergency communications are outlined as part of a project for the Office of Investigations, which is supported through TIGTA's mission, and TIGTA conducts a continuity of operations plan for headquarters-level exercises and existing policies for cybersecurity. Finally, the DOJ reported that its strategic plan does not outline emergency communications goals, strategies, or timelines.

Federal departments and agencies should continue to strive to include emergency communications as part of their strategic plans. This will ensure emergency communications strategies can be approached proactively and collaboratively across all disciplines.

Strategic plans are not regularly updated

In 2023, the ECPC identified that some FCEB agencies make infrequent updates to their strategic plans. Strategic plans which are not refined on an annual or bi-annual basis can become quickly outdated, limiting the accuracy and relevancy of emergency communications goals,

¹¹ DHS, Emergency Communications System Lifecycle Planning Guide. <https://www.cisa.gov/safecom/funding>.

strategies, and timelines contained within. For example, the DOS’s most recent update to its strategic plan took place due to a public health emergency and does not have a regular review schedule. Although the DOI’s Field Communications Modernization Strategic Plan was last updated in May 2022, the Department commits to updating its plan as the enterprise environment requires. Similarly, USSS updates its plan as needed, based on program evolution, though no regular cadence is adhered to.

In accordance with the DHS Resilience Framework, per a memorandum from the Undersecretary of Management, dated March 2018, requiring components to submit Plans for Resilience to OCRSO bi-annually, beginning in August 2019. Strategic plan updates should be made in similar cadence with component resilience plans as a point of ensuring communication technology infrastructure updates and redundancies are addressing any vulnerabilities for continual operability while adapting to mission needs.

The lack of consistent revisions to strategic plans may impede FCEB agencies from keeping pace with the evolution of threats and technologies pertinent to emergency communications. Federal departments and agencies and their stakeholders can mitigate risk by establishing a more regular or frequent cadence for revisiting and updating their strategic plans to ensure goals and priorities are aligned with present-day threats.

Successes



Agencies which address emergency communications within strategic plans made progress toward closing gaps outlined in strategic plans

In 2023, some FCEB agencies reported a healthy focus on closing emergency communications gaps as part of their strategic plans. A majority of agencies did not address emergency communications within strategic plans. Those which did demonstrated an impressive focus on tackling documented gaps. While these gaps are dynamic and everchanging, it is an encouraging trend that agencies are allocating resources to address critical gaps in a timely fashion as part of their strategic plans.

The Federal Aviation Administration (FAA) reported its Recovery Communications Program is completing a ten-year renewal cycle with a mechanism for assessing communications needs and gaps to update equipment such as satellites. At the end of 2023, the FAA launched a robust policy update for their emergency management team, which included a rewrite of the Crisis Management Handbook. This Handbook acts as the emergency management plan with overt delegated authority and incident-specific items, including cybersecurity.

Within DHS, the Federal Law Enforcement Training Center’s (FLETC) Director established a high-priority strategic pursuit called Workforce Care. This effort included the implementation of new early-warning communications systems which alerts staff of severe weather and other emergencies, remedying a compliance gap within the Center’s severe weather policy. CBP also took action to address an emergency communications gap impacting law enforcement officers, which was outlined in its strategic plan. CBP completed an initial evaluation of over 500 hotspot devices which automatically transmit location data via satellite when the user is in a communication dead zone to provide law enforcement officers situational awareness and improve safety while in austere environments. CBP developed a follow-on contract that allows

for additional devices to be purchased, with the goal of resolving this law enforcement officer communication vulnerability. Finally, USCG noted the lack of a standard PTT cellphone application was identified as a gap in its strategic plan, and the Coast Guard Office of C4 and Sensor Capabilities (CG-761) conducted an operational analysis and is actively working with stakeholders to construct a solution. If the gap was not included as part of USCG's strategic plan, it is unlikely to have garnered enough attention and priority to command resources for a solution.

Federal agencies that include emergency communications within their strategic plans should continue documenting and addressing gaps. Agencies which fail to target emergency communications gaps within strategic plans cannot expect the same level of attention or allocation of resources dedicated to them as agencies which prioritize the documentation of their communications gaps.

 *There are robust risk management strategies in continuity and recovery plans*

In 2023, FCEB agencies reported a variety of robust and routine risk management strategies such as communications assessments, training, testing, and exercises incorporated into plans for the continuity and recovery of emergency communication systems. Including risk management strategies in continuity and recovery plans is crucial to ensuring the resiliency and security of emergency communications systems across the nation. Departments and agencies must be able to depend on emergency communications to function properly in any event or scenario, and risk management techniques are the first line of defense in this regard.

USDA stated that it incorporates risk management principles into their Continuity Program Management cycle with risk tolerance and mitigation measures being assessed and developed in the pre-incident phase and not during the execution of the plans. USDA uses several risk management tools ranging from simple assessments of programs to more involved risk assessments of IT systems. DOL and GSA both reported conducting routine tests and exercises of their communications plans, allowing them to quickly identify gaps and shortfalls before they begin impacting mission operations. GSA's continuity and recovery plans also mandate independent communication exercises to ensure interoperability and resilience, serving as an additional layer of risk mitigation. Thus, regular testing and exercising of communications plans serves as a risk mitigation technique and helps to ensure continuity of communications.

Within DHS, the USCG reported following the planning process within Joint Requirements and Integration Management System (JRIMS), which incorporates risk management strategies. The JRIMS process begins by identifying capability gaps and potential risks, including factors such as technical issues and resource constraints. Identified risks are then assessed and prioritized based upon their projected severity and likelihood, which allows USCG to construct mitigation tactics such as developing a new solution or documenting requirements to combat those risks during the planning process. Meanwhile, FEMA's ONCP Integrated Public Alert and Warning System (IPAWS) shared that they contract with survey companies to test national emergency level alert capabilities every two years and plan improvement steps based on the results. In doing so, FEMA demonstrated its willingness to bring in independent, third-party contractors to support risk mitigation as part of their planning process, which is assured an objective, unbiased perspective and helped them to construct a thorough picture of their risk landscape.

Departments and agencies have demonstrated integrating an impressive level of risk management in plans for the continuity and recovery of emergency communication systems. Departments should continue incorporating testing, strategizing, and training consistently as part of their continuity and recovery plans to mitigate risks to emergency communications systems and safeguard their resiliency.

 *There was continued collaborative pre-incident communications planning*

FCEB agencies reported collaborative processes when conducting pre-incident communications planning throughout 2023. Agencies demonstrated a willingness to partner across the FSLTT landscape to adequately plan in various localities, which is crucial for ensuring interoperability during the event itself.

For example, DOJ reported that FSLTT relationships are consistently leveraged in pre-incident planning depending on the event and location. Other departments and agencies are included on a need-to-know basis, and the dynamics vary greatly across the more than 350 agreements and systems around the nation. Such a large volume of agreements indicate that DOJ was committed to collaborating with a wide variety of partners and localities based on the nature of the pre-incident planning. Similarly, FPS shared that it collaborated in pre-incident planning through coordination with state and local jurisdictions and participated in memoranda of agreement (MOA) to achieve interoperability. Formal agreements in the pre-incident communications planning phase shows FCEB agencies have an appetite and ability to partner effectively to prepare for incidents appropriately.

The FCC stated that operations teams conduct pre-incident assessments by conducting roll call scans to establish a baseline perspective of what the communications environment should look like in a specific area. These assessments also serve to identify any suspicious or nefarious signals. The FCC then shares the pre-incident scan information back to the multi-agency coordination center (MACC). This information is needed for all coordinating entities to test potential sources of interference and it demonstrates the FCC's willingness to collaboratively share information and mitigate interference possibilities during pre-incident planning. The FCC also provides spectrum management and deconfliction support to FSLTT emergency management personnel for National Special Security Events (NSSE) or Special Event Assessment Rating (SEAR)-1 events and provides staff to the MACC, the Critical Infrastructure Coordination Center, or applicable emergency operations centers to direct FCC field staff to mitigate communications issues. The FCC's amenability to surge staff to support coordination centers during special events should be recognized as a valuable collaboration strategy that ensures pre-incident planning is executed with readily available perspectives from communication experts.

FCEB agencies should continue pursuing collaborative relationships, agreements, and processes when conducting pre-incident communications planning. Engagement with FSLTT partners has proven to be necessary for proper pre-incident communications planning and federal agencies should continue collaborating with local authorities to optimize planning and interoperability.

LOOKING AHEAD:
Planning and Procedures Recommendations for
Federal Departments and Agencies



1. Federal agencies should include details about mandates, timelines, and inspections as part of their emergency communications standard procedures to ensure emergency communications strategic plans are being updated, exercised, and implemented regularly and effectively
2. Federal departments and agencies should carefully integrate emergency communications priorities into their strategic plans to ensure adequate priority, attention, and resources can be dedicated to the domain

Training, Exercises, and Evaluation

ASA Definition: Programs during steady-state operations to improve communications skills, test capabilities, and assess an organization’s progress towards interoperability goals¹²

Corresponding NECP Goal 3: 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

Many federal departments and agencies are still seeking their new normal after the impacts of the COVID-19 pandemic, including recruitment and retention challenges and the move to hybrid work environments. While organizations continued to adapt throughout 2023, FCEB agencies provided flexibility to meet the ever-changing workforce demands to ensure personnel received proper training, participated in planned exercises, and conducted evaluations. Without many communications-related deployments for federal agencies in 2023, federal agencies were able to successfully collaborate in other ways and leverage their new and existing partnerships.

Challenges and Priorities

 *Departments and agencies have varying approaches to the return to in-person trainings following the COVID-19 pandemic*

The COVID-19 pandemic has had a lasting impact on the way federal departments and agencies operate. Some entities have returned to in-person operations, while others have fully embraced virtual workspaces, with others somewhere in the middle. Many ECPC member agencies reported staffing to be challenging in 2023, and some shared that offering the option of virtual work has allowed them to hire and retain quality personnel. As new operational policies were shaped, federal departments and agencies also reviewed the benefits and challenges of in-person trainings and exercises.

Most federal agencies utilized the hybrid workspace for emergency communications training opportunities. Partners such as the FCC, TSA, USDA, USCG, DOJ, and GSA all conducted hybrid options to perform some or all their training. FLETC reported that while they offered

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

100% of their training in-person, much of the refresher or entry-level training courses could be completed virtually. DOI also shared that hybrid operations are now integrated into their continuity of operations (COOP) plan and annual trainings.

In 2023, FEMA conducted its annual continuity and biennial devolution exercises and granted the partaking DHS components maximum flexibility to determine participation requirements. After components experienced difficulties in performing tasks in previous years, DHS opted to increase in-person participation during these exercises to ensure accountability of on-site personnel. Additionally, it was determined components had improved their ability to conduct continuity and devolution operations in a mixed environment of virtual and in-person staff due to excessive pre-incident preparation and rehearsals.

As federal entities continue to navigate the ever-changing work environment, they should continue to implement virtual options where possible to increase cost-effectiveness and staff flexibility, while also implementing in-person opportunities as needed. Advancements in technology make service delivery more convenient, but the nature of emergency communications often requires some in-person collaboration and operations.

Departments and agencies lack communications-focused trainings

Federal departments and agencies continued to express the need for communications-focused trainings. While they are diligent in taking part in valuable exercises, many reported that none of their training is focused exclusively on communications-related material. The Department of Health and Human Services (HHS) and others reported participating in tabletop exercises such as Cyber Storm; however, none of these trainings give federal departments and agencies the opportunity to focus specifically on communications. TIGTA reported that communications personnel are often included after-the-fact and highlighted this as an area of improvement moving forward.

Emergency communications are critical to the efficacy and security of planned and unplanned incidents. In the 2022 ASA, it was reported that federal agencies made progress in including communications performance in their after-action reports, but in 2023, many continue to struggle with communications-focused training and exercises and including communications personnel during the planning stages of their trainings. Inclusion of communications personnel in the planning and execution of trainings and exercises, like COOP, and primary, alternate, contingency, and emergency (PACE) plans, can ensure plans are accurate, holistic, and efficient.

Communications Unit Leader (COML) positions are rare across the federal landscape

COML, a position under the Logistics Section of the Incident Command System (ICS), has responsibilities including: (1) developing plans for the effective use of incident communications equipment and facilities; (2) managing the distribution of communications equipment to incident personnel; and (3) coordinating the installation and testing of communications equipment.¹³ Across the federal landscape, these valuable and important positions are rare. Some departments

¹³ CISA, The Communications Unit Leader: A Valuable Resource for Incident Commanders, July 2011. https://www.cisa.gov/sites/default/files/publications/comlbrochure07_19_2011_0%25282%2529.pdf.

reported only having one individual fill this position and it is usually in addition to their regular duties. TSA representatives reported they have one COML-trained person in their entire component. USDA has many Communications Technicians, but these roles are secondary to their day-to-day responsibilities. Federal entities reported that it is difficult for personnel to retain the knowledge and skills learned during these trainings and there is a lack of follow up support for those who have completed the training. Due to these challenges, the FEMA Emergency Management Institute is revisiting the COML course and partnering with CISA to update the training. In 2023, TREAS reported having the opportunity to employ a COML position; however, other departments and agencies struggle to make this a reality.

During the 2023 data collection interviews, federal departments and agencies shared the importance of these roles but found it difficult to allocate personnel and time to commit to these responsibilities. Some agencies, such as USCG, host multiple trainings per year but are limited to their own personnel. Federal agencies may find success in sharing their resources and opening their training offerings to other federal, and even SLTT partners. This would allow agencies to continue to strengthen their pre-event relationships and fulfill the need for this important skill during unplanned and emergency events.

Successes



NSSEs were successful opportunities for training, exercise, evaluation, and collaboration

Federal partners strive to support and administer communications-specific training and exercise programs to improve emergency responders' proficiency with communications equipment. When trainings are not regularly scheduled or offered, consistent participation in planned events strengthens response to unplanned events. While there were not many opportunities for emergency communications-based deployments and responses in 2023, federal departments and agencies found that NSSEs, such as the State of the Union (SOTU) and large-scale sporting events, were successful opportunities for operational exercise and collaboration. The FCC supported NSSEs such as the SOTU, Presidential Addresses, and SEAR-1 events, including the Super Bowl. Two days before the February 2023 Super Bowl in Glendale, Arizona, a private company prematurely turned on a bi-directional antenna prior to having it inspected. This caused a disruption of public safety communications over a 200 square mile radius of the antenna, impacting communications supporting the SEAR-1 event. Within two hours of the disruption, the FCC, along with other response partners, were able to locate the source of the interference and restore communications. The local fire chief reported during a similar event, it had taken them over two months to locate and resolve the source of interference. For each major event the FCC participates in, a thorough documentation including strengths, areas for growth, and weaknesses is conducted, and issues which are identified will be addressed as part of a corrective action plan.

Federal departments and agencies continue to be intentional as it relates to communications testing for NSSEs. CISA, the FCC, and others have already begun planning for the 2028 Los Angeles Olympics and the 2026 Fédération Internationale de Football Association (FIFA) World Cup. These events and exercises continue to provide forums for successful pre-incident collaboration with FSLTT partners and provide responders with the opportunity to test available technologies and information sharing tools. In addition to communications-specific trainings, departments and agencies should continue to utilize real-world events to enable federal

responders to identify gaps in capabilities, provide an optimal level of emergency response, coordination, and collaboration.

Exercises continued to test federal readiness and continuity

National exercises involving many federal agencies are essential for validating progress toward promoting and sustaining a prepared nation to respond to catastrophic events. Events such as Eagle Horizon and Cyber Storm allow federal partners to test operational capabilities, evaluate policies and plans, familiarize personnel with roles and responsibilities, and foster meaningful interaction and communication across the emergency communications ecosystem.

In 2023, the FCC, TREAS, DOT, TSA, DOL, and multiple other interview participants cited the 2023 Eagle Horizon as a successful exercise to test their agency's COOP by deploying to remote locations to perform essential functions. The objectives included:

- Examining and validating the capabilities of FSLTT governments to take coordinated and inclusive protective actions prior to a major natural disaster;
- Demonstrating and assessing the ability to conduct post-event operations;
- Conducting inclusive recovery planning activities;
- Demonstrating the ability to implement continuity plans and perform essential functions;
- Examining and validating the capabilities to support long-duration power outages and critical interdependencies.

In addition to Eagle Horizon, FCEB agencies continuously and consistently trained and exercised their primary and alternate sites beyond the national level. DOT staff tested their communications at their alternate site monthly to ensure all equipment was working properly and staff were familiar with equipment and off-site operations. The FCC has an alternate site with the ability to virtually replicate emergency communications capabilities, which are frequently tested and continue to provide value. DOL, including the Mine Safety and Health Administration (MSHA), has found it tremendously effective to test and exercise with staff across the nation, such as the devolution site in Dallas, Texas, and the National Mine Health and Safety Academy, located in Beckley, West Virginia, as it opens the pool of staff available to partake in their emergency response group.

Departments and agencies should continue testing, training, and evaluating their continuity abilities alongside other federal organizations to identify areas of improvement, potential collaboration, and enhance emergency communications.

2023 Emergency Alert System (EAS) Nationwide Test

On October 4, 2023, FEMA in coordination with the FCC, conducted a nationwide test of the EAS and Wireless Emergency Alerts (WEA). WEA is a public safety system which allows customers of participating wireless providers who own compatible mobile devices to receive geographically targeted, text-like messages alerting them of imminent threats to safety in their

area.¹⁴ The test message was sent nationwide via WEA to cellular phones and over EAS to radios and televisions. The testing process was designed to evaluate the effectiveness of the FEMA public alert and warning systems to distribute an emergency message nationwide and the operational readiness of the infrastructure for distribution of a national message to the public.¹⁵ All the cellular carriers that participated in WEA received the alert on the day of the test, and the EAS test alert was successfully processed and made available to broadcasters, cable providers, and other communications services that participate in EAS.

The WEA system is an essential part of America's emergency preparedness. Since its launch in 2012, the WEA system has been used more than 84,000 times to warn the public about dangerous weather, missing children, and other critical situations—all through alerts on compatible cell phones and other mobile devices. FEMA will be conducting a survey on the WEA portion of the 2023 test to capture information about the geographic reach of the WEA Alert Message. Survey results will help FEMA and other WEA stakeholders, such as the FCC and public safety officials, enhance and expand WEA even further.

LOOKING AHEAD:
Training, Exercises, and Evaluation Recommendations for
Federal Departments and Agencies



1. Federal departments and agencies should strive to keep detailed records of communications-focused exercises and lessons learned to ensure that challenges and gaps are addressed
2. Federal agencies should share resources and open trainings to other federal and SLTT partners to strengthen their pre-event relationships and improve communications during unplanned and emergency events

¹⁴ FCC, Wireless Emergency Alerts, September 2023. <https://www.fcc.gov/consumers/guides/wireless-emergency-alerts-wea>.

¹⁵ FEMA, National Emergency Alert Test Results, October 2023. <https://www.fema.gov/press-release/20231004/national-emergency-alert-test-results>.

Communications Coordination

ASA Definition: Operational processes that enhance interoperable communications during incident response activities¹⁶

Corresponding NECP Goal 4: 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 communications coordination relies on federal departments and agencies knowing and sharing information about their emergency communications capacities with partners across all levels of government. Awareness of available emergency communications assets and resources from partner agencies impacts communications coordination and the ability for federal agencies to respond successfully during critical incidents and planned events. In 2023, the ECPC found some federal departments and agencies struggled to consistently implement NIMS or faced challenges in retaining NIMS trained personnel. Departments and agencies continued to work together to share communications systems and infrastructure, leading to enhanced coordination, effective use of public safety communications resources, and improved communications coordination and interoperability. Sharing resources not only improves communications coordination but can help public safety organizations from all levels of government achieve operable, interoperable, resilient, and secure communications.

Challenges and Priorities

 *Some federal departments and agencies continue to struggle with implementing NIMS*

NIMS is a comprehensive, nationwide systematic approach to incident management with a core set of doctrine, concepts, principles, terminology, and organizational processes for all hazards. It guides all levels of government, nongovernmental organizations, and the private sector to work together to prevent, protect against, mitigate, respond to, and recover from incidents. In 2023, some federal departments and agencies struggled to consistently implement NIMS, which provides stakeholders across the community with shared vocabulary, systems, and processes that guide personnel in working together during incidents.


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

The DoD attempted to implement NIMS for planned events but noted incorporating NIMS for unplanned events or war times proved difficult. The DoD reported it also lost its funding to continue NIMS training over a period of years. TIGTA follows NIMS guidance but did not have the opportunity to consistently employ NIMS during response operations in 2023. However, they expressed a desire to improve training and are prepared to use NIMS when needed. USSS has limited operations routinely using NIMS and ICS.

Other federal departments have NIMS-trained personnel but face turnover and challenges with tracking personnel trained on NIMS. For the FPS, the current rate of staff turnover and lack of available instructors for NIMS/ICS implementation has made it difficult to consistently employ and train to the ICS processes, methods, and structures. As an alternative, FPS provides NIMS briefing materials and ICS handbooks for reference. These materials highlight the ICS goals, the National Preparedness System, and the ICS organization. Despite these personnel and training challenges, all FPS plans are structured to meet the NIMS/ICS standards.

DHS components have been directed to formally adopt NIMS through their own directive processes, which would leverage existing emergency managers and planners to implement training, credentialing, or certification of personnel for Incident Management Training (IMT)-use. However, there is currently no DHS enterprise database for IMT qualification, making quick assessment of human capabilities across the department impossible. This creates difficulties for DHS to find the closest available and qualified personnel, regardless of component affiliation, to respond to an immediate disaster. Formally implementing NIMS enhances interoperability of communications and information management in incident response, and standardized resource management procedures promote streamlined coordination among different jurisdictions and organizations.

Successes

 *Federal departments and agencies implemented or explored sharing communications systems and infrastructure; however, work remains*

In 2023, multiple federal departments and agencies worked together to share communications systems and infrastructure, leading to enhanced coordination and effective usage of public safety communications resources. ICE shared infrastructure with FPS, FLETC, the Supreme Court of the United States, United States Marshal Service, and U.S. Citizenship and Immigration Services. Since 2016, when ICE began deployment of the San Francisco trunked land mobile radio (LMR) system, all new ICE systems were designed to be shared and interoperable with other federal agencies. Another example of systems and infrastructure sharing was DOI collaborating with USDA to deploy the FireNet network environment, a cloud-based solution specifically designed for FSLTT multiagency collaboration in a wildfire event and response, allowing users to chat, share files, and hold meetings in a secure team environment.

Federal departments and agencies reported difficulty with emergency communications budgeting in 2023. Exploring shared communications infrastructure or equipment could assist departments and agencies with the cost of implementation, maintenance, and upgrades. Sharing these resources and capabilities improves federal interoperability and improves fiscal responsibility.

Work remains in this area, though federal departments and agencies can continue to see improvements in operations and interoperability with increased collaboration and partnership.

 *Interoperability and sharing agreements with FSLTT and other emergency communications partners continue to grow*


In 2023, federal agencies continued to engage FSLTT partners in sharing communications systems and infrastructure, which led to improved communications coordination and interoperability. FLETC developed successful sharing agreements with local entities, as seen with the FLETC MOA with Eddy County, New Mexico. This MOA included an agreement for specific equipment, shared frequencies, and mass notification services. FLETC hopes to see similar improved coordination in Glynn County, Georgia, where they have started discussions about sharing specific equipment and shared frequencies.

The National Park Service (NPS) took steps towards communications improvements through new memoranda of understanding (MOU) with Rockingham and Page Counties in Virginia for multi-band radios for law enforcement and emergency medical services response. NPS is also pursuing an MOU with Madison County, Virginia, which would result in better interoperability in the Shenandoah Valley area.

While strides have been made to expand sharing agreements, partnerships with local entities have also faced challenges in local disaster response. These difficulties have spawned from various items, including lack of training from local staff unfamiliar with their disaster needs. To help bridge the lack of training gap, FLETC staff have been serving as mentors and helping with the professional development of FSLTT partners regarding emergency management. FLETC plans to continue this process in the future until needs are met by local partners.

NTIA reports that Emergency Support Function 2-Communications (ESF2) entails weekly telephonic meetings with the Communications Information Sharing and Analysis Center (COMM-ISAC) for situational awareness and when needed during disasters as the federal government expert and authority for federal frequency assignments. ESF2 would assist with assignment of frequencies in times of emergencies and interference resolution. DHS leads ESF2. The ESFs are sector coordinating bodies, activated selectively in emergencies. They include transportation, firefighting, public works, and others.

Federal agencies expanded interoperability and sharing agreements with FSLTT and other emergency communications partners and have laid the groundwork to expand and improve into 2024 and beyond.

 *Continued to implement resiliency and continuity of communications plans throughout operations*

In the field of emergency communications, resiliency and continuity are intertwined; resiliency is required to have continuity. Communications resiliency infers a network can withstand damages, thereby minimizing the likelihood of a service outage. It also indicates having a backup system(s), often referred to as redundancy, to withstand these potential outages. Continuity, often referred to as COOP, is the ability for emergency communications functions to perform,

regardless of any internal or external emergency or threat. Failure to have resilient emergency communications that allow for continuity of operations can result in the loss of life to both public safety and the public.

In 2023, continuity of communications plans were implemented throughout federal department and agency operations. For example, DOI used the Interagency Resource Ordering Capability (IROC) and had a National Interagency Incident Communications Division that supplied LMR equipment and frequencies within wildland fire operations for voice communications. In addition, DOI deployed the Nationwide Public Safety Broadband Network (NPSBN/FirstNet) devices to all type 1 and 2 teams as well as several dispatches across the nation via the IT Support Services Program. These capabilities and deployments are one example of how DOI complies with federal recommendations regarding high-value asset identification.

USDA OHS stated that USDA primary, alternate, and tertiary operations centers all utilize the PACE planning principles for communications as required by federal recommendations regarding high-value asset identification, to ensure communication systems remained operational during various circumstances, including emergencies, disruptions, and response operations throughout 2023.

The FCC also noted robust continuity plans and incident response capabilities. For example, its COOP plan complies with the high-value asset federal recommendations and is assessed bi-annually to identify and prioritize communications capabilities needed to ensure uninterrupted performance of its mission essential functions. The FCC was also deployed to support several natural disasters (e.g., hurricanes, tornadoes, wildland fires) as well as to NSSEs and SEAR-1 events, which were successfully supported due to thorough continuity planning. Maintaining robust COOP and resilience plans allowed federal agencies to provide emergency response support when needed.

LOOKING AHEAD:
Communications Coordination Recommendations for
Federal Departments and Agencies



1. Federal entities should continue to encourage the use of NIMS-compliant assets across the federal interagency landscape
2. Federal departments and agencies should continue to discover and pursue collaborative partnerships for shared emergency communications services which address roles, responsibilities, liabilities, spectrum, infrastructure, data interoperability, cybersecurity, and data sharing needs

Technology and Infrastructure


ASA Definition: Assets and equipment that support interoperability between different organizations, leverage partner resources for shared projects, and promote standards-based systems¹⁷

Corresponding NECP Goal 5: 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

Technology and infrastructure are the physical and digital assets that promote interoperable and continuous communications between partners during emergency incidents and day-to-day operations. In 2023, federal partners identified challenges in the transition and acquisition of emergency communications systems, as well as success in deploying novel communications technologies to improve interoperability. Federal and academic partners continued to find success in partnerships to accelerate research, development, testing, evaluation, and standards implementation for emerging technologies that improve emergency communications.

Challenges and Priorities

 *Transition to Next Generation 911 (NG911) across the federal landscape is inconsistent or non-existent*

Federal emergency communications stakeholders continue to transition their own networks to NG911 and provide supporting programs to assist NG911 initiatives by state and local 911 authorities, but consistency is disparate across the federal government or even non-existent in some departments or agencies.

Throughout 2023, USCG was assessing the requirements and opportunities to explore greater integration with NG911. Multiple factors affect USCG's needs and opportunities regarding NG911, including, but not limited to, the Coast Guard's unique maritime focus and the evolving nature of maritime distress calls, as well as the lack of jurisdictional agreements with existing public safety answering points (PSAPs). The requirement to operate within the Department of Defense Information Network, the availability of a DHS enterprise information sharing

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

capability, and the rapidly evolving enterprise architecture are additional challenges the Coast Guard must also consider.

For most of DOI's NPS dispatch centers, the upgrade to NG911 has not occurred, or it is not helpful due to the lack of cellular service in their response areas. While most of the NPS dispatch centers are secondary PSAPs without official 911 trunk phone lines, there are six NPS dispatch centers with 911 trunks, with five of those six having upgraded to NG911. NPS has identified multiple inhibiting factors, primarily infrastructure and technology (e.g., lack of dedicated 911 trunk lines at parks and a lack of NG911 systems), as well as funding. ICE TACCOM has not implemented NG911 in their dispatch center in Puerto Rico or for the FPS dispatch centers connected to the ICE TACCOM infrastructure.

Other federal government entities, including USDA, USSS, and CBP do not have 911 centers to transition to NG911. While some departments and agencies do not have 911 systems to upgrade, those with these critical systems should further investigate NG911 implementation to maintain communications with other FSLTT response agencies. Out-of-date 911 technology and a lack of authority can significantly impact the outcome of emergency incidents.

 *Federal emergency communications continue to be reliant on COTS equipment to support emergency communications missions*

In 2022 and 2023, federal departments and agencies reported using a variety of emergency communications systems to complete their public safety, disaster response, and emergency communications missions. These systems are often the most cost effective and robust way to support federal emergency communications missions; however, without the use of COTS solutions, FCEB agencies are left with limited options.

In 2023, USCG worked to implement internal solutions where practicable. However, when a shipboard interior communications capability gap presented a safety risk to the crew, additional COTS handheld radios were procured as a stop-gap solution for the identified deficiency, mitigating the threat facing the crew. In a year of numerous budget challenges across the federal government, DOJ utilized COTS products to improve operations and to close a budget-driven gap. Without these enhanced COTS capabilities, improved DOJ operations would not have been possible.

Emergency communications technologies and systems are often specialized and sourced from only a handful of commercial suppliers. This exposes the federal emergency communications enterprise to two distinct threats: supply chain attacks and supply-side shortages. While it is not feasible for the federal emergency communications enterprise to mitigate these threats completely, departments and agencies must evaluate and understand the risks to their emergency communications supply chains and build plans to ensure security and equipment lifecycles can be maintained. Federal departments and agencies should continue to seek up-to-date guidance regarding reliance on third-party infrastructure and equipment.¹⁸

¹⁸ CISA's [Secure by Design](#) program highlights the need for secure technology and equipment to ensure reliability and efficiency as it relates to emergency communications and beyond.

Successes

- ✓ Federal departments and agencies continued to prepare for significant investments into fifth generation (5G) capabilities

In December 2023, the FirstNet Authority Board approved investments to increase coverage on the network and accelerate FirstNet’s transition to a full 5G network. This investment follows the FirstNet Authority’s completion of validations and verification of the initial five-year buildout of Band 14 for public safety by the chosen network contractor. FirstNet serves 26,000 public safety agencies, with over five million connections, and the investment will accelerate the evolution of FirstNet’s 5G capabilities and ensure the network continues to deliver the innovation and reliability that first responders need.

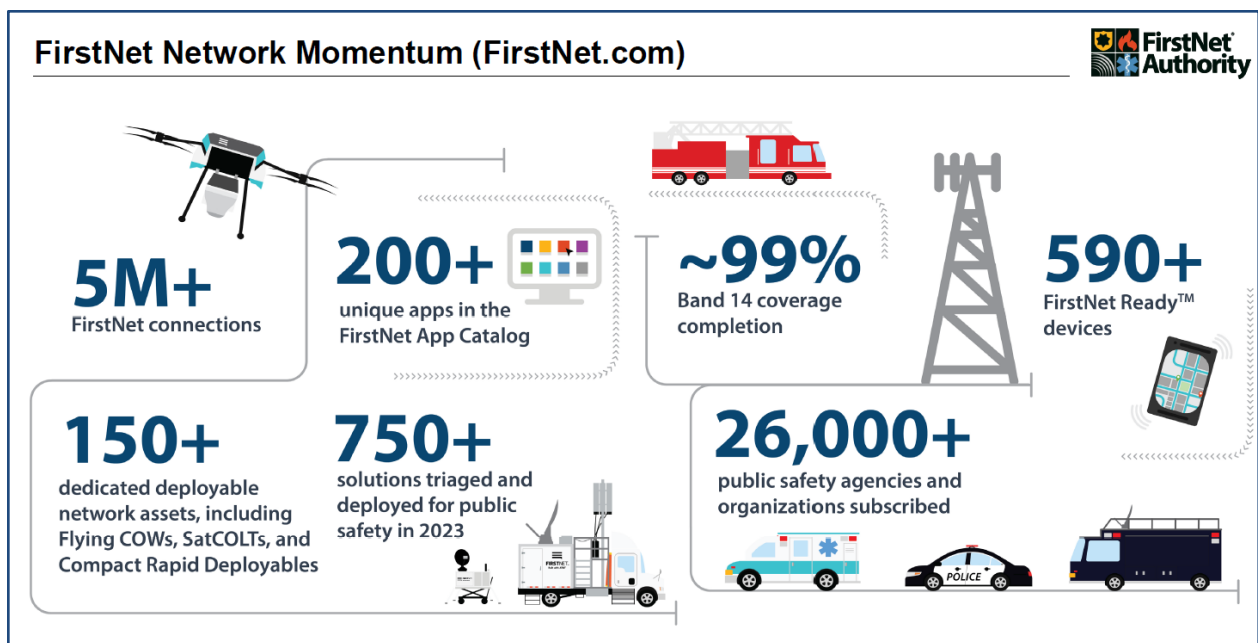


Figure 1: FirstNet Network Momentum¹⁹

DOJ utilized FirstNet and other 5G technologies, as they are continually evolving with spectrum and 5G for both voice and video. Several deployed FCC members also utilized FirstNet devices, where they are considered extended primary users and can request to be temporarily uplifted for priority on the 5G network during disasters or NSSE/SEAR events. The DoD deployed FirstNet capabilities with the G357 office for emergency management.


DoD stated the Army is looking to transition to 5G broadband for voice and data in areas where it is necessary, highlighting the fact that FirstNet’s Band 14 augments cell sites for a 5G solution. ICE TACCOM, in part, has leveraged 5G broadband voice and data for emergency communications interoperability as an augmentation to its LMR systems. Until 5G can meet mission critical PTT, ICE reported they will continue to use LMR as its primary means and 5G

¹⁹ FirstNet Authority, August 2023. <https://www.firstnet.gov/newsroom/events/firstnet-authority-combined-board-and-board-committees-meeting-august-2023>.

as an augmentation. One success DOJ highlighted was the use of FirstNet and PTT applications over broadband within one particular component. As technology evolves, DOJ is always testing to see how it can impact mission critical communications.

Continued investment into 5G capabilities will ensure agencies are taking advantage of beneficial emerging technologies and support the maintenance and modernization of federal emergency communications systems.

Finally, in May 2023, the FCC renewed FirstNet’s Band 14 license for another ten-year term, or for the remaining period of its authorization from Congress, whichever is sooner.

 *Federal partners are working cooperatively on research and development efforts to identify new technology solutions*

In 2023, NIST focused its research and development efforts on identifying new technology solutions to enhance emergency communications resiliency, cybersecurity, interoperability with existing systems or external partners, and continuity of communications.

NIST relied on several partners from research entities and commercial companies to push research and design efforts forward in 2023. Through a grant with Indiana University, NIST hosted the First Responder uncrewed aircraft systems (UAS) 4.0 Indoor Challenge, which focused on enhancing indoor use UAS for first responders’ situational awareness. The primary aim of UAS 4.0 was to improve UAS using video technology to effectively navigate an indoor environment and provide visibility and situational awareness to the Incident Commander prior to the entry of responders. These UAS solutions not only demonstrated great promise individually, but they also played a pivotal role in establishing a robust framework for live indoor testing and evaluation that can be replicated in future research endeavors. The data and insights yielded by UAS 4.0 hold the potential to propel UAS technology forward, delivering significant benefits to public safety initiatives, researchers, and the industry at large.²⁰ NIST has started conversations with Mountain View Fire Department in Colorado regarding a partnership to build a fire training center for local fire departments, which would also serve as a high-tech research facility for NIST’s Public Safety Communications Research (PSCR) and FirstNet Authority.

NIST and the FirstNet Authority partnered to create the Public Safety Immersive Test Center in Boulder, Colorado. Through this partnership, NIST’s PSCR Division and the FirstNet Authority continue to enable research and development, education, and training, by offering the facility at no cost to public safety agencies and organizations which support public safety response efforts, including private sector and academic institutions. The partnership and facility help answer key research questions around the future of user interfaces and location services for public safety training and operations.²¹

²⁰ NIST, September 2023. <https://www.nist.gov/news-events/news/2023/09/advancing-indoor-safety-first-responders-uas-40-indoor-challenge>.

²¹ NIST, May 2022. <https://www.nist.gov/news-events/news/2022/05/firstnet-authority-nist-launch-immersive-virtual-experience-center-public>.

The public safety community has placed an emphasis on accelerating research, development, testing, evaluation, and standards implementation for emerging technologies which improve communications and NIST's ongoing partnerships help reach those goals.

LOOKING AHEAD:
Technology and Infrastructure Recommendations for
Federal Departments and Agencies



1. Federal departments and agencies should evaluate the risks in emergency communications supply chains and build plans to ensure federal agencies equipment lifecycles can be maintained
2. Federal entities should establish dedicated lines of funding to support the maintenance and modernizations of federal emergency communications systems in accordance with their PACE plans for tactical, operational, and strategic emergency communications operations

Cybersecurity

ASA Definition: System and operational processes to secure communications capabilities against cyber threats²²

Corresponding NECP Goal 6: 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

Cybersecurity remains a top priority for federal departments and agencies across the nation. As cyber adversaries continue to increasingly target federal entities, especially those with emergency communications capabilities, federal entities continue to prioritize their cyber hygiene to ensure cyberattacks have limited impact. In 2023, departments and agencies reported challenges related to their specific organizations, but ultimately were successful in mitigating impacts of cyber-related events and sharing cybersecurity data with their FSLTT partners.

Challenges and Priorities

 *Departments and agencies are implementing cyber standards but continue to find agency-specific gaps*

Federal departments and agencies continue to prioritize the implementation of standards such as the NIST Cybersecurity Framework,²³ but they continue to find gaps as it relates to their unique organizations. USCG reported implementation of the NIST Cybersecurity Framework limited how information sharing is conducted internally and externally for their component. Some tribal, state, and local partners use applications which are no longer authorized on the USCG network, often making collaboration difficult. USSS reported they have experienced multiple challenges implementing increased Cybersecurity Framework suggestions, to include direct vendor, integrator, or manufacturer support, and there is limited USSS specialized staffing to support the dual generation systems for operations.

Cybersecurity is of utmost importance to all federal departments and agencies, particularly as technology and its associated risks continue to evolve. Some departments and agencies have begun the process of seeking outside, third-party commercial assistance in securing their systems and meeting the requirements of the current standards and best practices. Along with commercial

²² CISA, National Emergency Communications Plan, 2019. [cisa.gov/publication/national-emergency-communications-plan](https://www.cisa.gov/publication/national-emergency-communications-plan).

²³ NIST Cybersecurity Framework. <https://www.nist.gov/cyberframework>.

assistance, federal entities should consider seeking more tailored guidance from NIST and CISA to ensure that their systems are secure, protected, and operable.

 *Zero-Trust Architecture (ZTA) and Multi-Factor Authentication (MFA) implementation remain priorities, but progress varies across the landscape*

ZTA and MFA were significant to the federal government in 2023, though each department and agency seems to be at varying levels of completion. Following the *Executive Order on Improving the Nation's Cybersecurity*²⁴ issued in May of 2021, federal entities have expanded their modernization and cybersecurity efforts, citing increased benefits.

Some departments and agencies were significantly further along in their migration to MFA and ZTA in 2023, while others were still in the beginning stages. For example, the DOT made significant investments into MFA for their department, with an 80% completion rate reported in 2023. Their investment into this technology provided a solution for a long-standing accessibility issue reported by the FAA and has even been able to provide the DOT with visibility into their managed endpoints. Additionally, they were able to improve the number of assets running at the end-of-life or those with legacy software or systems.

In 2023, DOL began a two-year roll out to provide a variety of Zero Trust (ZT) solutions department-wide. This process included their emergency communications networks and was expected to take about four months to complete. DOL reported they expected to be 75% complete in 2024. Similarly, USDA expected to complete their ZTA implementation by the end of fiscal year 2024.

Others reported being early in their transition. For example, GSA reported they were about 30-40% of the way towards completion in 2023. TIGTA was also navigating the early maturity phase of ZTA implementation and had procured technology to begin micro-level segmentation, with plans for completion of this process by the end of 2024. While TIGTA reported the technology was ready for implementation, their policy development was still in its infancy.

Executive guidance and industry best practices provide federal departments and agencies with the roadmap to implement ZTA and MFA into their day-to-day and even emergency operations. While each entity faces differing technological and cybersecurity-related challenges, guidance continues to evolve to meet their needs. Federal departments and agencies should continue to seek the most-up-to-date guidance to keep their systems secure.

Successes

 *FSLTT cybersecurity data sharing remains strong*

Federal departments and agencies are continuously and successfully sharing relevant cybersecurity data with FSLTT partners. This intentional and consistent sharing of information

²⁴ The White House, Executive Order on Improving the Nation's Cybersecurity 2021. <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>.

increases situational awareness and gives federal partners the opportunity to collaborate, while decreasing the scope and magnitude of cyber threats.²⁵

HHS in particular shared a significant amount of cyber-related information internally and externally in 2023. The Administration for Strategic Preparedness and Response (ASPR) distributes weekly and ad hoc bulletins, while the Healthcare Cybersecurity Coordination Center (HC3) provided information to public health agencies and even private sector partners to improve cybersecurity and provided: (1) awareness about threats impacting infrastructure, (2) mitigation techniques, (3) monthly briefing and vulnerability bulletins, and (4) sector alerts.

The DOI Cyber Intelligence Group shared cybersecurity threat information with FSLTT partners via e-mail communications, threat exchange partner calls, and in-person through their detailee with the Federal Bureau of Investigation (FBI) Cyber Task Force. DOI established relationships with other partner agencies to provide additional intelligence reporting, indicators of compromise, and open communication channels for continued collaboration.

Many federal departments and agencies reported proactively sharing cybersecurity-related information with CISA and highlighted the importance of having a federal partner with dedicated cyber authority. This is discussed in depth later in this report and federal entities should continue to prioritize the sharing of data with their FSLTT partners to increase awareness and decrease the impact of malicious threats.



Cyberattacks and threats were resolved quickly without detrimental impacts

As reported in 2022, federal departments and agencies continue to be targeted by malicious actors to disrupt day-to-day and emergency operations. Fortunately, the prioritization of cyber hygiene by federal entities was evident. While federal departments and agencies were impacted by cyberattacks and other malicious cyber events in 2023, the effects of these events were minimal.

DOJ experienced multiple breaches on their spectrum, PTT solutions, and Data Encryption Standard radios; however, these were all resolved quickly with minimal impacts. DHS components also experienced a wide range of issues, though none were damaging to their operations. FPS reported weather-related damages to their towers in the Sierra Nevada Mountains and USSS reported disruptions when a commercial circuit provider experienced cut lines, accidents, and storms. FEMA ONCP IPAWS experienced two systems outages in 2023 on the IPAWS Open Platform for Emergency Networks (OPEN) alert warning system. This was attributable to other DHS network disruptions. The total time between both disruptions resulted in 9.53 hours of inaccessibility to the IPAWS-OPEN system for FSLTT alerting authorities and caused the IPAWS Program to miss the IPAWS Key Performance Parameters of 99% Threshold and 99.9% Objective.

Federal departments and agencies continued to experience cyber-related events and outages, but their preparedness, vigilance, and resilience for these events lessened the impacts and decreased

²⁵ CISA. Information Sharing. <https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing>.

the efficacy of these events. Federal entities should continue to collaborate with FSLTT partners and vendors to ensure their systems are resilient and secure.

 *Federal entities continue to look to CISA for cybersecurity guidance*

As the national coordinator for critical infrastructure security and resiliency, CISA is designed for and dedicated to partnership and collaboration. CISA continues to be seen as an authority on cybersecurity guidance, best practices, and cyber hygiene. Several ECPC member agencies, including the FCC and DOI, noted the sharing of attack-related information with CISA and CISA's cyber-related guidance provided great value and coordination throughout 2023.

DOS coordinated with CISA and others successfully during the cyberattack on Microsoft Exchange Online²⁶ in June 2023. This intrusion impacted e-mail inboxes of the DOS, the Department of Commerce (DOC), and the United States House of Representatives, among others. Furthermore, DOS regularly received updates and alerts from CISA regarding possible cyber incidents. This coordinated effort between DOS, DOC, and CISA highlighted the importance of partnership across the cyber landscape.

DHS continued to promote this collaboration across its components. The ICE Investigations team shared network intrusion information with victims that fall into the 16 areas defined by CISA as the Critical Infrastructure Sectors,²⁷ including FSLTT partners.

DOL received threat information from their Security Operations Center (SOC) to enhance the CISA and Defense Information Systems Agency (DISA) information. Over the course of 2023, DOL discovered unemployment information had been published to the Dark Web. DOL responded quickly, working with state partners and CISA to ensure DOL systems had the proper protocols and mitigations in place to avoid attack. DOL reported working closely with CISA to share cyberattack information because of CISA's respected relationships with non-federal entities.

Other agencies such as USDA, HHS, and GSA coordinated with CISA regularly, sharing indicators of compromise and imperative cyberattack information. GSA coordinated with CISA and the National Security Agency on threat modeling for the design of important systems. These seamless opportunities for sharing and the proven guidance from CISA highlighted their role in securing the nation.

²⁶ CISA, March 2024. https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf.

²⁷ CISA, Cyber Infrastructure Sectors. <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors>.

LOOKING AHEAD:
Cybersecurity Recommendations for
Federal Departments and Agencies



1. Federal departments and agencies should seek tailored cybersecurity assistance from federal partners to ensure they receive specific and actionable guidance regarding industry standards and executive direction to keep their systems secure, operable, and interoperable
2. Federal departments and agencies should continue to share cybersecurity threat information with other FSLTT partners to continue building resilient relationships and identify potential threats within the federal cybersecurity sphere of responsibility
3. Federal departments and agencies should remain diligent in working with vendors to ensure cyber threats are identified and mitigated prior to serious cybersecurity breaches
4. Federal departments and agencies should continue to follow cybersecurity guidance as it relates to ZTA and MFA

IV. Conclusion

In 2023, federal agencies utilized the ASA to coordinate across all levels of government to provide an updated status on emergency response capabilities and operations supported by public safety communications capabilities. Federal partners worked towards increasing interagency and national emergency communications capabilities, using the NECP as a guide. While federal partners reported challenges to increased interoperability, they also demonstrated progress towards achieving the NECP goals, including:

- Maintaining strong interagency governance relationships ensuring effective coordination and decision-making and consistent inclusion of non-traditional stakeholders in communications governance processes;
- Incorporating robust risk management strategies within their continuity and recovery plans;
- Continuing to adjust to post-pandemic challenges, resulting in a varied approach in the return to in-person trainings;
- Testing operational capabilities, policies, plans, and personnel during real-world events and national exercises;
- Limiting impacts of malicious attacks and disruptions in 2023 due to increased prioritization of cyber hygiene practices;
- Expanding interoperability and sharing agreements with FSLTT and other emergency communications partners this year and laying the groundwork to expand and improve even more in 2024;
- Continuing to rely on COTS equipment for a variety of emergency communications systems to complete their public safety, disaster response, and emergency communications missions;
- Working cooperatively on research and development efforts to identify new technology solutions to enhance emergency communications resiliency, cybersecurity, interoperability with existing systems or external partners, and continuity of communications.

Moving forward, the 2023 ECPC ASA findings will help identify federal interagency priorities and develop future ECPC initiatives for improving interoperability and public safety communications. The ECPC recommends federal agencies consider the associated recommendations throughout their strategic planning processes to adequately address gaps and anticipate risks on the horizon. Doing so, agencies may better coordinate interoperability decisions and investments, enhance interoperability during response operations, and strengthen the ability of public safety at all levels of government to prepare for, respond to, and recover from disasters, acts of terrorism, and other emergencies.

V. Appendices

Appendix A: Abbreviations

| | |
|-------------------------|--|
| 5G..... | Fifth Generation |
| AI | Artificial Intelligence |
| ASA..... | Annual Strategic Assessment |
| ASPR..... | Administration for Strategic Preparedness and Response |
| BECS..... | Base Emergency Communications System |
| CBP..... | U.S. Customs and Border Protection |
| CIO..... | Chief Information Officer |
| CISA | Cybersecurity and Infrastructure Security Agency |
| CISR..... | Critical Infrastructure Security and Resilience |
| COML..... | Communications Unit Leader |
| COOP..... | Continuity of Operations |
| COTS | Commercial-Off-the-Shelf |
| COVID-19..... | Coronavirus Disease 2019 |
| DHS..... | Department of Homeland Security |
| DISA | Defense Information Systems Agency |
| DOC | Department of Commerce |
| DoD..... | Department of Defense |
| 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 |
| ECC..... | Emergency Communications Center |
| ECPC..... | Emergency Communications Preparedness Center |
| FAA..... | Federal Aviation Administration |
| FBI | Federal Bureau of Investigation |
| FCC..... | Federal Communications Commission |
| FCEB..... | Federal Civilian Executive Branch |
| FEMA | Federal Emergency Management Agency |
| FIC | Federal Interoperability Coordinator |
| FIFA..... | Fédération Internationale de Football Association |
| FirstNet | Nationwide Public Safety Broadband Network (NPSBN) |
| FirstNet Authority..... | First Responder Network Authority |
| FLETC | Federal Law Enforcement Training Center |
| FPIC | Federal Partnership for Interoperable Communications |
| FPS..... | Federal Protective Service |
| FSLTT..... | Federal, State, Local, Territorial, and Tribal |

GSA.....General Services Administration

HC3.....Healthcare Cybersecurity Coordination Center

HHS.....Department of Health and Human Services

IAB.....Integrated Advisory Board

ICE.....U.S. Immigration and Customs Enforcement

ICS.....Incident Command System

ICT.....Information Communications Technology

IMT.....Incident Management Training

IPAWS.....Integrated Public Alert and Warning System

IROC.....Interagency Resource Ordering Capability

IT.....Information Technology

JRIMS.....Joint Requirements and Integration Management System

JWPMO.....Joint Wireless Program Management Office

LMR.....Land Mobile Radio

MACC.....Multi-Agency Coordination Center

MFA.....Multi-Factor Authentication

ML.....Machine Learning

MOA.....Memoranda of Agreement

MOU.....Memorandum of Understanding

MSHA.....Mine Safety and Health Administration

MWCOG-DC.....Metro Washington Council of Governments

NCSWIC.....National Council of Statewide Interoperability
Coordinators

NECP.....National Emergency Communications Plan

NG911.....Next Generation 911

NIMS.....National Incident Management System

NIST.....National Institute of Standards and Technology

NPS.....National Park Service

NSA.....National Security Agency

NSSE.....National Security Special Events

NTIA.....National Telecommunications and Information
Administration

OCIO.....Office of Chief Information Officer

OHS.....Office of Homeland Security

OMB.....Office of Management and Budget

ONCP.....Office of National Continuity Programs

OPEN.....Open Platform for Emergency Networks

OSTP.....Office of Science and Technology Policy

OCRSO.....Office of Chief Readiness Support Officer

PACE.....Primary, Alternate, Contingency, Emergency

| | |
|--------------|---|
| PSAP | Public Safety Answering Point |
| PSCR..... | Public Safety Communications Research |
| PSHSB | Public Safety and Homeland Security Bureau |
| PTT | Push-to-Talk |
| | |
| R&D..... | Research & Development |
| | |
| SEAR | Special Event Assessment Rating |
| SLTT | State, Local, Tribal, and Territorial |
| SOC..... | Security Operations Center |
| SOTU | State of the Union |
| | |
| TACCOM | Tactical Communications |
| TIGTA..... | Treasury Inspector General for Tax Administration |
| TREAS..... | Department of the Treasury |
| TSA..... | Transportation Security Administration |
| | |
| UAS..... | Uncrewed Aircraft Systems |
| USCG..... | United States Coast Guard |
| USDA..... | United States Department of Agriculture |
| USSS..... | United States Secret Service |
| | |
| WEA | Wireless Emergency Alerts |
| | |
| ZT..... | Zero Trust |
| ZTA..... | Zero Trust Architecture |

Appendix B: Interview Participants

| Department or Agency | Component or Office |
|---|---|
| Department of Commerce | First Responder Network Authority |
| | National Institute of Standards and Technology |
| | National Oceanic and Atmospheric Administration |
| | National Telecommunications and Information Administration |
| Department of Defense | U.S. Army |
| | U.S. Marine Corps |
| Department of Health and Human Services | Office of Information Security |
| Department of Homeland Security | U.S. Customs and Border Protection |
| | Cybersecurity and Infrastructure Security Agency |
| | Federal Emergency Management Agency |
| | Federal Law Enforcement Training Center |
| | Federal Protective Service |
| | U.S. Immigration and Customs Enforcement |
| | Transportation Security Administration |
| | U.S. Coast Guard |
| | U.S. Secret Service |
| Department of the Interior | Office of Policy, Management, and Budget |
| Department of Justice | Office of the Chief Information Officer |
| Department of Labor | Mine Safety and Health Administration |
| | Office of the Assistant Secretary for Administration & Management |
| Department of State | Bureau of Diplomatic Security |
| | Diplomatic Continuity Programs |
| | Diplomatic Technology Bureau |
| | Operations Center |
| Department of Transportation | Federal Aviation Administration |
| | Federal Highway Administration |

| Department or Agency | Component or Office |
|---|---|
| | General Counsel's Office |
| | National 911 Program |
| | Office of the Chief Information Officer |
| | U.S. Maritime Administration |
| Department of the Treasury | Treasury Inspector General for Tax Administration |
| Federal Communications Commission | Office of the Chief Information Officer |
| | Public Safety and Homeland Security Bureau |
| General Services Administration | General Services Administration, Federal Acquisition Service, Office of the Information Technology Category |
| | Office of Mission Assurance |
| United States Department of Agriculture | Cybersecurity and Privacy Operations Center |
| | Office of the Chief Information Officer |
| | Office of Homeland Security |
| | United States Fire Service |

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 questions below represent the generic structure that guided each interview.

Governance and Leadership

1. In 2022, your department/agency reported using (governance group) for making emergency communications governance decisions. How often does the (governance group) meet and have there been any significant changes to the (governance group) structure or its function?
 - a. If your agency has made changes to the (governance group), how did the changes impact your department/agency's governance structure or affect interoperable communications in the last year?
 - i. What were your group's major successes, challenges, or other notable actions in 2023?
2. How would your department/agency describe its relationship with other federal partners? Does this relationship allow your organization to promote or enhance federal interoperability? What can be done to improve relationships at the federal level?
3. How does your department/agency prioritize funding needs for communications (e.g., allocations for communications systems, areas of investment, emerging technologies, systems to sustain)?
 - a. Has your department or agency performed a threat assessments or resource prioritization?
 - b. What are your department's current emergency communications priorities?
4. Does your department/agency incorporate input from internal stakeholders (e.g., end users, technical staff, and senior leadership)? From external partners (e.g., other federal entities, state, local, tribal, or territorial stakeholders)? If so, please explain how this is done.
 - a. Does your department or agency incorporate non-traditional stakeholders in your communications governance body or decision-making process (e.g., information technology staff, critical infrastructure providers, cybersecurity subject-matter experts)? If so, please explain how this is done.
5. Does your department/agency participate in any external governance bodies (e.g., SAFECOM, Federal Partnership for Interoperable Communications [FPIC])?
 - a. If yes, which one(s)? How has your department/agency benefited from participation in these groups?

Planning and Procedures

1. Does your department/agency's strategic plan outline emergency communications goals, strategies, and timelines?
 - a. If yes, how often do you implement updates to your department/agency's strategic plan? What factors influenced your decision to update (e.g., communications evaluations, after-action review, cyber incident, regulatory requirement, etc.)?

- b. If no, how does your department/agency measure progress against National Emergency Communications Plan (NECP) objectives and or the emergency communications needs for your department?
 - c. For agencies that have previously reported operating dispatch centers or emergency communications centers (ECCs), are your federal ECC personnel recognized as first responders? If so, what kind of impact has this had on hiring or retaining qualified communications personnel?
2. What emergency communications capability gaps did your strategic plan address in 2023?
 - a. What steps did your department/agency take to close those emergency communications gaps?
3. What is your department/agency's process for assessing current and future emergency communications needs (e.g., operability, interoperability)?
4. How does your department/agency conduct lifecycle planning to inform your organization's funding decisions?
 - a. Are there any barriers preventing your agency from conducting life cycle planning?
5. What types of risk management strategies (e.g., communications assessments, training, testing or exercises, incident response strategy, mitigation, and redundancy) does your department/agency incorporate into plans for continuity and recovery of emergency communication systems?
6. How does your department/agency conduct pre-incident communications planning for both planned (e.g., National Special Security Events (NSSEs), multi-jurisdictional local/regional events) events and incidents (e.g., emergency response, natural disasters)?
7. How does your department/agency balance sustainment of existing communications systems/technologies with building new communications capabilities?
 - a. How does your department/agency balance expansion of existing communications systems/technologies while sustaining legacy communications capabilities?

Training, Exercises, and Evaluation

1. Did your department/agency continue to augment training and exercise events with virtual environments or was there a return to in-person activities? How effective was each training? Share any gaps and successes.
2. How many communications-focused exercises (e.g., in-person or virtual) did your department/agency participate in?
 - a. What communications successes or challenges did your department/agency identify by participating? How did your department/agency incorporate communications interoperability and resiliency into continuity of operations planning/exercises?
 - b. Were your communications-focused exercises external or internal to your department/agency?
 - c. If your department/agency did not, what were the barriers preventing you from participating in communications-focused exercises? How did your department/agency test communications readiness and incorporate lessons learned or after-action report (AAR) findings?
3. Did your department/agency identify any technical or operational capability gaps as a

result of training/exercise engagements?

- a. If yes, does your department/agency formally evaluate (e.g., AARs, action summary report) training or exercises and document lessons learned? How did your department/agency notify leadership, follow-up with recommendations, incorporate improvements, include training, and implement enforcement to close the capability gap(s)?
 - b. If no, how does your department/agency evaluate communications capabilities gaps during training/exercises and how are challenges identified and remediated?
4. How did your organization update your training and exercise programs to account for emerging technologies (e.g., Fifth Generation [5G], Next Generation 911 [NG911], public safety broadband)?
 - a. How did your organization update your training and exercise programs for new communications capabilities (e.g., push-to-talk applications, new communications systems)?
 5. How does your department/agency evaluate communications gaps identified (e.g., AAR, action summary report) through training or exercises and how is the progress to remedy the gaps tracked?
 - a. Does your department deploy an implementation plan to remediate the communications gaps and challenges identified?
 - b. How did your department/agency assess the readiness of your organization's communications systems and personnel for both day-to-day and out-of-the-ordinary situations?
 6. How frequently were the performance of emergency communications systems and personnel included in AARs in 2023?
 - a. What are some of the challenges or reasons for not including communications in AARs?
 7. How often are emergency communications section personnel incorporated into agency mission or operational focused exercise planning and at what stage of the planning process are the communications personnel included?

Communications Coordination

1. The National Incident Management System (NIMS) guides all federal departments and agencies, nongovernmental organizations, and the private sector to work together to prepare, prevent, protect, mitigate, respond, and recover from actions during planned events and incidents. Does your department/agency consistently employ and train to the Incident Command System (ICS) processes, methods, and structures?
 - a. If no, how does your department/agency ensure the effective coordination and usage of all available communications capabilities during planned events and incidents?
 - b. Does your department/agency utilize Communications Unit Leader (COML) or Information Technology Service Unit Leader (ITSL) positions within ICS?
 - c. Are there any challenges or recommended improvements for NIMS you would like to share?
2. Provide a few examples when your department/agency partnered with federal, state, local, tribal, or territorial (FSLTT) partners during response operations in the past year.

- a. How does your department/agency ensure communications resources (e.g., personnel, equipment, infrastructure) readiness for multi-agency/multi-jurisdictional response operations for both planned events and incidents?
3. How did your department/agency ensure operability, interoperability, real-time information sharing, and continuity of communications during response operations and did you encounter any challenges maintaining reliable interoperable communications?
4. From your department/agency perspective, did you establish new or update existing formal written agreements (e.g., memoranda of understanding/agreement, inter-agency agreements) with FSLTT partners that define roles and responsibilities during response operations?
 - a. If yes, what new or updated formal written agreements did you establish with FSLTT partners and did the defined roles and responsibilities impact response operations?
 - b. If no, has there been discussion within your department/agency to establish formal agreements with FSLTT partners? What factors prevent forming formal agreements?
5. How does your department/agency maintain and share information securely on the current status of their primary, alternate, contingency, and emergency (PACE) communications capabilities both internally for the agency and in real-time with FSLTT partners?
6. Has your department/agency implemented or explored shared communication systems and infrastructure?
 - a. Does your department/agency have ongoing sharing agreements (land mobile radio networks, data networks, communications facilities, repeater and receiver sites, towers, etc.) in place with FSLTT and other emergency communications partners?
 - i. If so, with whom do you have ongoing sharing agreements?
7. Does your department/agency actively participate in the Emergency Communications Preparedness Center's (ECPC) Federal Resource Sharing Working Group? If not, can you share your department/agency's perspective and what you think can be leveraged to encourage participation?

Technology and Infrastructure

1. Has your department/agency engaged in any research and development efforts to identify new technology solutions to enhance emergency communications resiliency, cybersecurity, interoperability with existing systems or external partners, or continuity of communications?
 - a. If yes, what was the solution and what impact did it have on your department's emergency communications systems?
2. How does your department/agency stay in compliance when incorporating communications standards or frameworks (e.g., Project 25 [P25], National Emergency Numbers Association [NENA] i3, National Institute of Standards and Technology [NIST] Cybersecurity Framework, 3rd Generation Partnership Project [3GPP], Zero-Trust [ZT] Framework)?
3. How often did your department/agency implement internal solutions to close a capability gap?

- a. What was the risk or capability gap that led your department/agency to utilize the solution?
4. Which groups or partners (e.g., private, non-governmental organizations, FSLTT partners) did your department/agency collaborate with to conduct new communications technologies research and development projects?
5. For agencies that have previously reported operating dispatch centers or ECCs, what kind of impact has NG911 had on your department/agency ECCs or dispatch centers?
 - a. How does your organization assess NG911 maturity across your 911 infrastructure?
 - b. Are there any factors that inhibit the transition to NG911? If your organization does not utilize NG911 or maintain ECCs, how does your department/agency assess and respond to emergency calls on lands/facilities administered by your organization?
6. Has your department/agency incorporated emergency electric vehicles into its vehicle fleets?
 - a. If yes, were there any challenges installing or operating standard emergency communications equipment? Were you able to mitigate these challenges? If so, how?
7. Has your department or agency leveraged machine learning, unmanned aerial systems (UAS), or artificial intelligence (AI) in emergency communications technologies?
 - a. If yes, what challenges and/or limitations did you experience regarding human infrastructure (e.g., staffing, training)?
8. Has your department or agency leveraged AI in emergency communications when appropriate?
9. Has your department/agency transitioned to 5G broadband for voice or data? If so, how has it impacted your emergency communications interoperability capabilities?

Cybersecurity

1. What has your department/agency done to share cyberattack information (e.g., e-mail updates, partner meetings, IT department communication) with other FSLTT partners? What benefits did sharing cybersecurity information provide to your department/agency?
 - a. Are there barriers hindering better cybersecurity information sharing (e.g., classification, routers, switches, networking requirements, culture)?
 - b. How have you worked with others in your cybersecurity planning?
 - c. Does your department/agency share near-real-time cyberattack information?
 - d. How does your department/agency implement Criminal Justice Information Services (CJIS) guidance with regards to reporting, response, and recovery functions?
2. Does your department/agency's current communications strategic/operational planning process include a cybersecurity incident response plan?
 - a. If no, how would your organization respond to a cybersecurity incident that impacted emergency communications systems?
 - b. If yes, how is this plan communicated and trained into your organization?
 - c. Does your department/agency have separate cybersecurity incident response and cybersecurity vulnerability plans? Or are these documented in a singular plan?
3. Does your department/agency have a physical or cyber security risk assessment process?

- a. If yes:
 - i. Did your department/agency's risk assessments identify any emergency communications equipment or system-specific physical or cybersecurity vulnerabilities? How did your organization address emergency communications equipment or systems vulnerabilities?
 - ii. How frequently do risk assessments occur?
- b. If no:
 - i. If your department/agency does not have a security risk assessment process, then how does your department/agency assess physical or cybersecurity risks?
 - ii. What are the barriers to conducting regular risk assessments?
4. What types of disruptions to emergency communications has your department/agency experienced within the last year during response operations (e.g., radio-frequency jamming, interference, solar flares, downed towers)?
 - a. What steps were taken to mitigate the disruption(s)?
5. Per Executive Order 13800, each agency head shall use the Framework for Improving Critical Infrastructure Cybersecurity, or any successor document to manage the agency's cybersecurity risk. How has the use of the Framework, or similar standards, impacted emergency communications interoperability?
 - a. Has your organization identified any challenges impacting emergency communications as a result of the use of the NIST Cybersecurity Framework?
6. How does your department/agency assess the cyber resiliency of its emergency communications systems (e.g., risk assessments, exercises, penetration testing, after-action reports)? [Note: 'cyber resiliency' is the ability of a network to withstand an attack, or continue to function under the strain of an attack]
7. On a scale of 1-5, how do you rate the maturity of your organization's Zero-Trust Architecture (ZTA) implementation? And why?
 - a. Who in your organization is responsible for ZTA implementation?
8. Does your department/agency have any additional cybersecurity concerns regarding your emergency communications systems?
9. For agencies that have previously reported operating dispatch centers or ECCs, what cybersecurity barriers prevent your ECC from collaborating with other FSLTT ECCs? Do you have any plans to leverage vendor solutions e.g., public key infrastructure certificates to communicate with other ECC's?

Appendix D: ASA Alignment to 2016 Government Accountability Office Findings

In 2016, the Government Accountability Office (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.

GAO found the Emergency Communications Preparedness Center's (ECPC) collaborative efforts improved coordination and information sharing among federal emergency communications programs. However, GAO identified an area for improvement in that the ECPC does not actively track its member agencies' implementation of ECPC recommendations. 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, GAO recommended that the ECPC institute a mechanism to track ECPC members' implementation of recommendations.

Through tailored interviews, the Annual Strategic Assessment (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 the National Emergency Communications Plan goals and objectives (e.g., establishing a department-wide Interoperability Coordinator). As explained 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 the implementation of ECPC recommendations. The ECPC has included within the 2023 ASA a tracking mechanism, **Summary of 2023 ASA Findings and Recommendations**.