Emergency Communications Preparedness Center: Annual Strategic Assessment

Calendar Year 2022 Report to Congress

October 24, 2023

Homeland Security

Cybersecurity and Infrastructure Security Agency (CISA)

Message from the Director

October 24, 2023

On behalf of the Cybersecurity and Infrastructure Security Agency (CISA) Emergency Communications Preparedness Center (ECPC), I am pleased to submit to Congress the 2022 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 element of effective public safety communication, the ECPC identified common challenges and priorities, as well as successes.

Throughout 2022, agencies continued to face an environment of challenges shaped by the Coronavirus Disease of 2019 (COVID-19) pandemic; constraints on financial, spectrum, and physical infrastructure resources; cyber and infrastructure threats; and continued transition to new communications technologies that require new approaches to training, security, and operations. These challenges, and how federal agencies continued to respond to them, determined the ability of the federal agencies to coordinate resources and effectively maintain steady-state and emergency response and advance interoperability and resilience of emergency communications throughout 2022.

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 Cathy McMorris Rodgers
Chairwoman, House Committee on Energy and Commerce

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

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

The Honorable Rand Paul
Ranking Member, Senate Committee on Homeland Security and Government Affairs

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

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

Sincerely,

Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency

Executive Summary

The Emergency Communications Preparedness Center (ECPC) was established by 6 United States Code § 576 to improve interoperable and operable communications coordination among federal agencies. The ECPC is comprised of 14 federal agencies who meet regularly to address gaps in emergency responders' and key decision makers' abilities to communicate across jurisdictions and functions. Pursuant to authorizing statutes, the ECPC developed the Annual Strategic Assessment (ASA) to evaluate and report to Congress the Federal Government's interoperability with appropriate partner agencies and the impact of coordination on continuity of communications and interoperability during day-to-day operations and 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/emergency preparedness personnel to operate during steady-state and emergencies. Doing so allows responders to maintain situational awareness, coordinate response efforts, and share mission-critical information. The Federal Government plays a key role in addressing challenges and improving the effectiveness of emergency communications. Collectively, FSLTT agencies have a responsibility to coordinate efforts to enhance interoperability, reduce costs, and strengthen and maintain relationships with agencies from all levels of government.

The 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 vulnerabilities, successes, and next steps needed to move closer to accomplishing each goal of the NECP to mitigate risk.[2]

The 2022 ECPC ASA documents communication efforts during coordinated response 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 2022, the ECPC found that federal agencies continued to leverage emerging technologies, interagency relationships, and strong governance structures to ensure the operability and interoperability of emergency communications. Federal agencies approached interoperable communications from multiple angles, including:

[1] CISA, National Emergency Communications Plan. cisa.gov/necp.

[2] Ibid

- Continuing to maintain strong and persistent governance structures by including non-traditional emergency communications personnel in intra-agency governance decision-making bodies;
- Maintaining and deploying well established continuity of operations (COOP) plans to include Primary, Alternate, Contingency, and Emergency communications planning, preparation and testing/exercising;
- Conducting after-action reviews to document successes and opportunities for improvement in trainings, exercises, and events;
- Sharing resources between FSLTT partners to improve connectivity and interoperability;
- Deploying emerging technologies to enhance communications operability and resilience; and
- Maintaining and testing the security and confidentiality, integrity, and availability of communications networks.

More information on these key findings can be found in Section III Summary of 2022 ASA Findings and Recommendations.

2022 Annual Strategic Assessment

Contents

Message from the Director i
Executive Summary iii
2022 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 2022 ASA Findings and Recommendations 4
IV. Analysis 7
Governance and Leadership 7
Challenges and Priorities 8
Successes 10
Planning and Procedures 12
Challenges and Priorities 12
Successes 14
Training, Exercises, and Evaluation 16
Challenges 16
Successes 18
Communications Coordination 21
Challenges 21
Successes 23

Technology and Infrastructure 25
Challenges and Priorities 26
Successes 27
Cybersecurity 29
Challenges and Priorities 30
Successes 31
V. Conclusion 35
VI. Appendices 36
Appendix A: Abbreviations/Definitions 36
Appendix B: Interview Participants 40
Appendix C: ASA Interview Questions 42
Governance and Leadership 42
Planning and Procedures 42
Training, Exercises, and Evaluation 43
Communications Coordination 44
Technology and Infrastructure 45
Cybersecurity 45
Appendix D: ASA Alignment to 2016 Government Accountability Office Findings ... 47

I. Statutory Language

6 United States Code (U.S.C.) § 576[3] 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 2022 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 interoperability and the ability of public safety response providers to continue to communicate in the event of disasters, acts of terrorism, other man-made disasters, and planned events. The ECPC leveraged principles from the National Emergency Communications Plan (NECP) and the SAFECOM Interoperability Continuum[4] to develop the 2022 ECPC ASA.

[3] 6 U.S.C. § 576 sets forth the establishment, operation, and function of the Emergency Communications Preparedness Center (ECPC).

[4] CISA, Interoperability Continuum: A Tool for Improving Emergency Response Communications and Interoperability. 2021. cisa.gov/safecom/resources.

II. Scope and Methodology

As administrator of the ECPC, the Cybersecurity and Infrastructure Security Agency (CISA) developed the 2022 ECPC ASA with input and coordination from federal agencies.[5] 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. By compiling best practices and lessons learned, this assessment serves as 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 2022 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 2022 ECPC ASA findings align to the NECP goals[6] and the SAFECOM Interoperability Continuum[7], providing a common framework for identifying challenges, trends, and lessons learned.

Data Collection Approach

In 2022, the ongoing COVID-19 pandemic resulted in the continuation of virtual operations for the majority of the Federal Government. 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 the 2019 summit, federal agencies shared their individual ASA-related data, while also collaborating with other federal stakeholders to identify trends and other common challenges and solutions. Recognizing the benefits of these past data collection methods, for the collection of 2022 data, CISA combined the two approaches, conducting eleven two-hour virtual interviews with individual ECPC member agencies and hosting a virtual and in-person collaborative interagency summit in March of 2023.

For each departmental interview, CISA tailored approximately 50 interview questions, which were aligned to the NECP strategic goals and individualized for each of the departments and agencies with the intent of gathering detailed information on emergency communications

[5] 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).
[6] To meet these goals, the updated NECP establishes 19 objectives, each with success indicators, for the continued improvement of emergency communications for the nation. CISA, National Emergency Communications Plan. 2019. cisa.gov/necp.
[7] CISA, SAFECOM Interoperability Continuum Brochure. 2021. cisa.gov/sites/default/files/2022-12/21_0615_cisa_safecom_interoperability_continuum_brochure_final.pdf

challenges and successes at the department or agency level. The interview questions were based on open-source research and responses from previous ASA interviews.

Data Analysis Approach

In support of the 2022 ECPC ASA, CISA gathered extensive qualitative notes from federal agency interviews, ASA Summit activities, and follow-up outreach and interviews. CISA utilized the interviews and ASA Summit data collected to assess federal coordination and success towards achieving the NECP goals and recognize potential areas of opportunities for improvement.

III. Summary of 2022 ASA Findings and Recommendations

The following tables provide a summary of the 2022 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: 2022 ECPC ASA Key Findings

SECTION	KEY FINDING
Governance and Leadership	1. Lack of resources, e.g., staffing and funding, present challenges for federal departments and agencies to implement a Federal Interoperability Coordinator 2. Federal departments and agencies wish to strengthen the ECPC to enable better decision making with leadership and support greater access and advocacy to senior-level decision makers across the government 3. Emergency communications governance groups continue to incorporate non-traditional stakeholders into decision making processes
Planning and Procedures	1. Federal departments and agencies continued to face challenges implementing lifecycle planning to support public safety communications systems 2. Federal departments and agencies regularly review plans and policies based on established schedules 3. Risk mitigation strategies such as succession planning, recovery plans, and formal evaluation varies widely throughout the federal enterprise
Training, Exercises, and Evaluation	1. Federal agencies transitioned to hybrid training to complete training needs with some use of in-person training. Hybrid training was considered successful, although some agencies still prefer in-person training 2. Processes for the development of after-action reports (AAR) and tracking of emergency communications improvements varies widely throughout the Federal Government
Communications Coordination	1. Departments continue to show a strong level of federal collaboration in response to planned and unplanned events 2. Federal department and agencies continue to explore shared communications systems and infrastructure 3. Relationships with state, local, tribal and territorial (SLTT) partners remain strong both in steady-state and response operations

SECTION	KEY FINDING
Technology and Infrastructure	1. Federal departments and agencies continue to transition to Next Generation 911 (NG911) technologies, but face continued challenges with the prioritization of NG911 resources in budget planning 2. The Federal Government is highly reliant on commercial-off-the-shelf (COTS) emergency communication equipment and systems 3. Federal departments and agencies with emergency communications missions and resources piloted and implemented innovative technologies for emergency communications uses, but more research could be conducted
Cybersecurity	1. Federal departments and agencies continue to encounter difficulty interoperating with SLTT due to SLTT's continuing transition from the Data Encryption Standard (DES) to the Advanced Encryption Standard (AES) 2. Zero-trust maturity for emergency communications varies widely across the Federal Government 3. Cybersecurity threat information is shared, but classification of information can limit access 4. Federal departments and agencies are uniformly concerned about the vulnerability of mission critical emergency communications systems

Table 2: 2022 ECPC ASA Recommendations

SECTION	RECOMMENDATIONS
Governance and Leadership	1. Federal agencies should aim to strengthen governance by establishing and maintaining internal agency central coordination points or decision-making bodies to lead the management and administration of emergency communications operability and interoperability 2. Federal agencies should continue to find ways to implement a Federal Interoperability Coordinator (FIC) position to ensure progress towards national interoperability
Planning and Procedures	1. Establish formal emergency communications plans and procedures that guide federal agency deployment of resources and technologies to achieve interoperable communications 2. Federal agencies must use documented formal risk mitigation strategies against physical, cyber-related, response, and attrition risks in emergency communications to minimize disruptions to critical communications 3. Explore establishing adequate funding mechanisms, for example, a multi-year approach, to improve lifecycle planning management

SECTION	RECOMMENDATIONS
Training, Exercises, and Evaluation	1. Federal agencies should strive to rebuild/re-introduce in-person emergency communications training, exercises, and other educational engagements to assist in building institutional knowledge and key relationships within the Federal Government 2. Federal emergency communications specific job descriptions should be created, modified, and shared as needed to enhance retention, specialized training, and career opportunities within the Federal Government
Communications Coordination	1. Continue to encourage the use of National Incident Management System (NIMS) compliant emergency communications assets across the Federal Government 2. Discover collaborative partnerships for shared federal emergency communications services that address roles, responsibilities, liabilities, spectrum, infrastructure, data interoperability, cybersecurity, and data sharing needs
Technology and Infrastructure	1. Evaluate the risks in emergency communications supply chains and build plans to ensure that federal agencies equipment lifecycles can be maintained 2. Develop federal standards or a roadmap for the integration of electric vehicles (EV) in mission critical, emergency communications, and public safety transportation fleets to streamline the transition from internal combustion vehicles 3. Establish dedicated lines of funding to support the maintenance and modernizations of federal emergency communications systems
Cybersecurity	1. Federal agencies should identify SLTT partners in need of assistance in migration to Advanced Encryption Standard (AES) encryption and direct them to the appropriate resources, grants, and other technical assistance 2. Federal agencies should continue to research and deploy resiliency measures to ensure operability and connectivity of mission critical communications systems 3. Federal agencies should communicate, develop, and share best practices to speed implementation and solve shared challenges related to the deployment of zero-trust architectures in their emergency communications networks 4. Federal agencies should continue to follow established cybersecurity standards, such as those provided by the National Institute of Standards and Technology (NIST), and investigate how to ensure all emergency communications needs align with cybersecurity best practices

IV. Analysis

Emergency Communications Defined

The means and methods for exchanging information necessary for successful incident management[8]

The 2022 Emergency Communications Preparedness Center (ECPC) Annual Strategic Assessment (ASA) examined major events impacting continuity of communications and interoperability, and the six National Emergency Communications Plan (NECP) strategic goals, including: **(1) Governance and Leadership; (2) Planning and Procedures; (3) Training, Exercises and Evaluation; (4) Communications Coordination; (5) Technology and Infrastructure; and (6) Cybersecurity**. The following pages contain a summary of findings and spotlight successes and challenges in federal emergency communications coordination in 2022.

Governance and Leadership

ASA DEFINITION: Coordination and decision-making processes that guide interoperable communications priorities and policy

CORRESPONDING NECP GOAL 1: Develop and maintain effective emergency communications governance and leadership across the Emergency Communications Ecosystem[9]

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 emergency communications interoperability challenges, strategic planning, training, and exercise strategy, and to benefit from policy improvement. In 2022, federal agencies identified several gaps within departments and agencies; specifically, the lack of resources to support Federal Interoperability Coordinators (FIC) within departments and components, inconsistent emergency communications governance maturity, and the lack of governance authority of the ECPC. Despite these challenges, federal agencies continued to improve their governance models through inclusion of non-traditional emergency communications staff in governance groups, maintenance of strong interagency relationships, and balancing the sustainment of new and existing communications capabilities.

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

[9] CISA, National Emergency Communications Plan. 2019. cisa.gov/publication/national-emergency-communications-plan.

Challenges and Priorities

Lack of Resources for Federal Interoperability Coordinators (FIC)

Interoperability ensures consistent and coordinated emergency planning and response. To guarantee interoperability is maintained throughout agencies and within the federal community, Cybersecurity Infrastructure Security Agency (CISA) and the NECP have recommended the implementation of FICs at each ECPC member department or 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 2022, federal agencies reported no planning efforts to implement a department-wide FIC due to a lack of resources (e.g., funding, staffing, etc.) and reported fulfilling the duties of this position by other means. For example, the Department of Justice (DOJ) explained it did not have current plans to implement a full time FIC as the agency does not have adequate staff or resources to support the position. Although DOJ noted not having the capacity to designate a lead division to manage interoperable emergency communications challenges and issues, the DOJ consolidates coordination and management of interoperability.

To contend with not having a FIC, some federal agencies and their components utilize alternative mechanisms to fill this need. For example, the United States Coast Guard (USCG) leverages the Department of Homeland Security's (DHS) Joint Wireless Program Management Office (JWPMO) to manage interoperability needs, and the Customs and Border Protection (CBP) takes advantage of a dedicated interoperability position within their cybersecurity office. Similarly, the Department of State (DOS) designates their Major Events Coordinator and the DOS Executive Secretariat to handle internal, external, and international emergency communications challenges. Identifying a central coordinator for incident response agencies can improve decision-making, partnerships, consistency, adaptability of federal communications programs and improve an agency's ability to respond in a coordinated manner with all levels of government, jurisdictions, disciplines, and organizations. As such, federal agencies should continue to find ways to implement a dedicated FIC position to ensure progress towards national interoperability[10].

Participation in the ECPC is Strong, but Enhanced ECPC Governance Needed

Interagency governance structures play a vital role in fostering collaborative relationships which enhance information sharing and better address challenges and issues related to emergency communications. The 2022 ASA discovered federal agencies continue to actively participate in the ECPC to maintain relationships and share information across multiple disciplines. Despite federal agencies' strong and enthusiastic participation in ECPC activities, some expressed a need for the ECPC to enhance its governance over the 14 member agencies and suggested the ECPC explore new ways to collaborate with decision makers and one another to address federal emergency communications topics. This request was notably highlighted by the U.S. Department of Treasury (TREAS) which advocated for increased engagement from the ECPC working

[10] CISA, National Emergency Communications Plan. 2019. cisa.gov/publication/national-emergency-communications-plan.

groups to contend with federal emergency communications and interoperability requirements and challenges. TREAS proposed utilizing the ECPC Working Groups to share more information with ECPC member agencies about the National Interoperability Field Operations Guide (NIFOG) to foster recognition and use of the guide. TREAS also described the need for the ECPC to be granted a stronger voice among the interoperable emergency communications community within the Federal Government to aid the support of national interoperability.

Other agencies expressed the need to leverage the ECPC to complete agency specific missions. The National Telecommunications and Information Administration (NTIA) benefits from continued participation in ECPC Working Groups and information shared by partner members. The First Responder Network Authority (FirstNet) also reported their continued participation in the ECPC to engage federal partners to identify, promote, and enhance interoperable communications with the goal of improving the National Public Safety Broadband Network (NPSBN). To better support and enhance interagency governance, federal agencies should continue to engage with the ECPC to highlight shared mission challenges. Additionally, the ECPC must enhance communication of these shared challenges to decision makers for visibility and action.

Ongoing Inconsistency of Intra-Agency Emergency Communications Governance Maturity

The level and structure of departmental emergency communications governance remained inconsistent among federal agencies in 2022, ranging from foundational to more mature models. Robust governance structures are essential for organizing emergency communications not only at the federal level, but at all levels of government. The ASA found that some federal agencies do not employ a central coordinating body and others leverage internal information technology management groups or external coordinating bodies for governance. For example, the Centers for Disease Control and Prevention (CDC), which is a component of the Department of Health and Human Services (HHS), independently manages upgrades, enhancements, and makes decisions for emergency communications. The Administration for Preparedness and Strategic Response (ASPR) of HHS plans to lay the groundwork for employing a central coordinating governance body by implementing the HHS Tactical Communications Operations Plan. However, due to institutional barriers, this body will be unable to oversee emergency communications governance for the entire department.

Some agency components oversee intra-agency governance across all sub-components. For example, the Treasury Inspector General for Tax Administration (TIGTA) which is a sub-component of TREAS, has been the decision-making body for land mobile radio (LMR) emergency communications, spectrum management, and interoperability since 2005. Other federal agencies, such as the DOJ, foster a combined information and communications technology approach for emergency communications governance through the Wireless Control Board (WCB) and their Technology Working Group (TWG). These groups review communications-related policy and funding requests, as well as coordinate emergency communications issues across the agency. While agencies like the Department of Labor (DOL) do not utilize a formal coordinating body, they instead participate in external governance groups to facilitate emergency communications decision-making.

Effective coordination and decision-making require a robust governance structure and processes designed to ensure accountability, inclusiveness, adaptability, and action for emergency communications. To enhance these structures, federal agencies should reference the *ECPC Federal Emergency Communications Governance Guide*[11] for recommendations on effective frameworks to address emergency communications interoperability, operability, and continuity challenges through improved resource coordination, partnerships and enhanced collaboration efforts.

Successes

Progress Towards More Well-Rounded Governance Models

In 2022, federal agencies reported efforts to establish more inclusive governance structures by adopting a more comprehensive coordinating body inclusive of information technology (IT) components. This model collectively expands the decision-making process in a positive manner to maintain full oversight of the information and communications technology ecosystem that is prevalent in the federal enterprise. For example, the General Services Administration (GSA) makes emergency communications governance decisions through the Information Technology Governance Board (ITAB), a subcommittee of the GSA Enterprise Management Board (EMB), which is responsible for defining an IT shared service strategy for GSA. The ITAB is also responsible for defining the technical direction for shared service delivery and approves IT funding requests. Through active engagement with the GSA Shared Service Portfolio teams, the ITAB approves strategies to reduce IT operational costs, increase efficiencies through enterprise-wide initiatives, improve service delivery, and standardize technology at GSA. Oversight of the ITAB is provided by the Deputy Chief Information Officer (DCIO) and periodically by the Budget Director when necessary to make budget-related decisions.

DOJ also fosters a combined information and communications technology model approach for emergency communications governance through the WCB and TWG to coordinate emergency communications issues across the department. Adoption of this adaptive governance approach throughout the federal departments and agencies could standardize addressing the evolution and convergence of traditional emergency communications systems with IT systems to meet the challenges that may arise out of the ever-evolving emergency communications ecosystem.

Agencies Maintain Strong Interagency Governance Relationships

Strong interagency relationships ensure effective coordination and decision making for federal emergency communications interoperability.[12] In 2022, several federal agencies discussed how informal partnerships enhance their emergency communications efforts. For example, the USCG shared that DHS agencies are very cooperative and collaborate monthly to discuss how to improve interoperability and/or provide any assistance across the enterprise. DOS highlighted its collaborative relationship with other government agencies (OGAs) which "promote the well-

[11] The *ECPC Federal Governance Guide* is available on the ECPC Max.gov portal

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

being of our citizens abroad with the help of OGAs." The ongoing ability for federal agencies to sustain and enhance governance relationships is critical to emergency communications operability and interoperability, effective interagency coordination and decision making and agency mission requirements. Additional guidance on governance can be found in the *2018 SAFECOM Emergency Communications Governance Guide for State, Local, Tribal, and Territorial Officials*.[13]

Leadership is Vital to Funding and Sustainment of Emergency Communications Systems

Federal agencies with strong governance and leadership advance emergency communications priorities and interoperability through communications investments. Enhancing emergency communications interoperability through these investments requires that federal agencies sustain existing communications needs while concurrently building new communications capabilities, resulting in more reliable and robust emergency communications systems. In 2022, federal agencies discussed how they balance communications needs and investments. TREAS prioritizes the sustainment of existing communications systems and technologies based on mission critical agency needs while also designating resources for projects identified through their planning and future mission requirements. TREAS relies on TIGTA to monitor communications vendor upgrades and technological advancements then reports and discusses with TREAS bureaus and leadership about how best to balance emerging technologies with mission requirements.

Additionally, the United States Department of Agriculture (USDA) manages governance of licensing and sustainment needs through the Office of the Chief Information Officer (OCIO). This top-level leadership approach ensures that emergency communications receive the necessary updates, patches, and systems access on demand when needed. However, the U.S. Army (USA) leverages governance coordination of communications investments through the Base Emergency Communications System (BECS) Program, allowing them to better protect funding for sustainment and refreshing of public safety communications capabilities to improve interoperability. When federal agencies have an effective governance or leadership approach that prioritizes the management and administration of emergency communications systems and services investments, agencies can successfully and strategically promote National interoperability projects and resource needs.

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

1. Federal agencies should aim to strengthen governance by establishing and maintaining internal agency central coordination points or decision-making bodies to lead the management and administration of emergency communications operability and interoperability
2. Federal agencies should continue to work to find ways to implement a FIC position to ensure progress towards national interoperability

[13] CISA, 2018 SAFECOM Emergency Communications Governance Guide for State, Local, Tribal and Territorial Officials. 2018. cisa.gov/resources-tools/resources/governance-documents

Planning and Procedures

ASA DEFINITION: Formal documents that detail department or agency interoperable communications objectives, progress indicators, and day-to-day operational processes, plans, and procedures to guide the deployment of resources and technologies

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[14]

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 that guide the deployment of resources and technologies, as well as strategic and multi-year plans that guide continuity and resilience goals of agencies. In recent years, these plans have been integral to the flexibility and sustainment of federal emergency communications. In 2022, federal agencies noted that they were able to update these plans to handle the emergency communications landscape following the Coronavirus Disease of 2019 (COVID-19) pandemic. However, it was also noted that the Federal Government could improve emergency communications equipment lifecycle and risk mitigation plans to strengthen overall federal preparedness.

Challenges and Priorities

Emergency Communications Lifecycle Planning Challenges Remain

Lifecycle planning requires public safety agencies at all levels of government to assess needs, hazards, risks, and threats regularly to preempt changes in requirements and technological evolution.[15] Lifecycle planning also aids federal agencies to plan long-term investments in interoperability solutions and maintenance costs. In 2022, several agencies expressed challenges in the emergency communications lifecycle planning process. For example, the Department of Interior (DOI) described that the Federal IT Acquisition Reform Act requires them to have strong investment management at the agency level. As a result, the DOI Chief Information Officer (CIO) executes governance over all major IT investments, including radio communications. This governance structure often limits input from field and operational personnel, which ultimately causes lifecycle plans to poorly reflect operational needs. There are also federal agencies, such as

[14] CISA, National Emergency Communications Plan. 2019. cisa.gov/publication/national-emergency-communications-plan

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

the CDC that do not have any documentation outlining their emergency communications goals, strategies, or timelines, making it difficult to track the lifecycle management of communications assets. To mitigate challenges with lifecycle planning, federal agencies should reference resources such as the *2018 Emergency Communications System Lifecycle Planning Guide*[16] which provides additional guidance regarding public safety communications system lifecycle planning. The document is intended to guide readers on how best to fund, plan, procure, implement, support, and maintain public safety communications systems, and eventually to replace and/or dispose of outdated system components.

Inconsistent Standards for Risk Mitigation Planning

By operating emergency communications systems, public safety agencies at all levels of government face systemic risks (e.g., cyber-attacks, data breaches, system failures, etc.). Federal agencies that implement risk mitigation plans for these types of associated risks minimize the possibility of the loss and/or difficulty with recovery of emergency communications systems. In 2022, the ECPC found varied approaches to federal agencies' implementation of risk strategies such as succession planning, formal evaluations, system testing, and general risk mitigation planning. For example, agencies such as CBP hold regular meetings to assess the current and potential communication risks for their communications systems. Also, as part of the Commission's risk mitigation strategy plan, the Federal Communications Commission (FCC) employs plug out exercises to test and manage the loss of connectivity to communications circuits to better identify associated risks.

Other formally planned risk mitigation strategies employed by federal agencies include GSA's use of a dispersion strategy that aligns with the Federal Mission Resilience (FMR) Strategy,[17] and ties into the agency's continuity plans and recovery of communications systems. The USCG has a plan through the Joint Requirements Integration and Management System (JRIMS) to incorporate risk management strategies for communications systems. While all these risk mitigations systems are effective, there is no single consistent federal standard. To fully mitigate risks to emergency communications, federal agencies must use documented formal risk mitigation strategies against physical, cyber-related, response, and attrition risks in emergency communications allows for agencies to minimize disruptions to critical communications.

Prioritization of Emergency Communication Planning Continues, But Work Remains

Emergency communications planning is a key element in assisting federal agencies to better prepare for the deployment of emergency communications resources, effectively coordinate with public safety agencies from different levels of government and maintain critical operations. In 2022, the ECPC identified that federal agencies prioritized emergency communications as part of the formal planning process through continuity of operations (COOP) plans, standard operating procedures (SOPs) and allowing internal agency components or bureaus to manage their own plans. For example, DOI has their own Field Communications Modernization Strategic Plan,

[16] CISA, 2018 Emergency Communications System Lifecycle Planning Guide, 2018. cisa.gov/safecom/funding

[17] Federal Mission Resilience Strategy. Executive Office of the President, 2020. hsdl.org/c/abstract/?docid=848323

while DOI bureaus have complimentary strategies specific to their operational area of responsibilities. Also, agencies such as GSA use the National Continuity Policy (NCP) and SOPs to outline emergency communications goals, strategy, and timelines. The USCG prioritizes emergency communications planning by employing the USCG Incident Management Handbook,[18] NIFOG,[19] and the Homeland Security Presidential Directive (HSPD) 5,[20] which discloses the whole of government national level interoperability. TREAS allots emergency communications planning latitude to their bureaus, as they run their own communications systems and dictate their communications documentation procedures.

In addition to the formal planning processes identified above, there are federal agencies such as NTIA and FirstNet that also rely on their own individual COOP plans. While some federal agencies have improved upon ensuring formal written strategies, plans, and procedures that guide emergency communications are in place, work remains to ensure all federal agencies adopt a full comprehensive emergency communications plan.

Successes

Scheduled Review Cycles of Communications Plans Remains Consistent

Federal agencies that set a pre-determined timeline for reviewing emergency communications plans and strategies have proven to better document their overall emergency communications vision. Benefits of this scheduled review include better prioritization of communications resources, strengthened governance structures, the identification of future communications investments, and the resolution of long-standing operability and interoperability issues.[21] In 2022 DOS reported updating their strategic plans on a continual basis. DOS uses a Change Management Board and working groups to review and approve any service impacting change on a reoccurring schedule. Throughout 2022, the USCG reviewed their plans after every exercise or training event. Other agencies such as the Federal Law Enforcement Training Centers (FLETC), the DOT Federal Transit Administration (FTA) and DOJ review their emergency communications plans annually. In addition, FTA reviews its COOP plans quarterly, while DOJ also reviews its *Mission Critical Communications Strategy* annually. Agencies should continue to designate timeframes for reviewing emergency communications planning given the rapidly evolving emergency communications ecosystem to address the evolution of associated risks. To strengthen formal, written guidelines or instructions for emergency communications during normal operations and incident response, agencies should visit the SAFECOM Resource Standard Operating Procedure website.

Updating Emergency Communications Plans Generates Added Benefits

[18] USCG, USCG Incident Management Handbook. 2019. homeport.uscg.mil/Lists/Content/DispForm.aspx?ID=60118&Source=/Lists/Content/DispForm.aspx?ID=60118

[19] CISA, National Field Operations Guide. 2021. cisa.gov/resources-tools/resources/nifog

[20] DHS, Homeland Security Presidential Directive 5. 2003. dhs.gov/publication/homeland-security-presidential-directive-5

[21] CISA, National Emergency Communications Plan. 2019. cisa.gov/publication/national-emergency-communications-plan

Throughout 2022, the ECPC found that federal agencies benefited from reviewing and updating emergency communications plans, providing a positive impact towards emergency communications capabilities.

The Defense Information Systems Agency (DISA) was also able to address several interoperability concerns during their planned review of emergency communications, including ensuring appropriate system integrations, setting up legacy public safety gateways (LPG), the ability to turn off selective routers, and strategic or tactical plans (i.e., if DoD is notified that a state is transitioning to Next Generation 911 (NG911), DoD must act quickly to ensure system adaptability for interoperability and remain mobile to install an LPG).

As part of DOT FTA's 2022 emergency communications planning efforts, the agency reviewed and updated their COOP plans as continuity of communications capabilities and equipment is required to be replaced or upgraded as part of scheduled refresh cycles. This prevented disruption to their emergency communications system as equipment reached its serviceability threshold for operational use or malfunction. Agencies that maintain scheduled review updates not only address operability and interoperability issues but allow for the discovery of other potential benefits which can address improvement to interoperability, integration of new communications technologies, and sustainment of current capabilities.

Evaluation of Communications Needs Enhances Interoperability

To better address future emergency communications priorities and needs, federal agencies regularly evaluate their communications needs and capabilities. Agencies deployed various mechanisms, governing bodies, and methods to help with facilitating program evaluation efforts. The ability for agencies to routinely evaluate and plan for the long-term strategy of emergency communications guidance can bolster the effectiveness and overall mission capabilities of the federal enterprise. In 2022, DOJ reported that they evaluated their current and future communications needs through discussion and data collection from their component and field levels, WCB, and TWG. Additionally, DOI reported using their Field Communications Improvement Executive Leadership Team (FCIELT) to assist in evaluating current and future communications needs. USDA also leveraged their CIO to work with mission areas and collect data to assess the best and most robust solution for ensuring coverage and compatibility within the USDA communications network. Both USCG and the FLETC conduct operational analysis annually for their communications evaluation needs, while DOS continuously evaluates new and emerging communications systems to determine their impact and/or interoperability with existing communications systems. Rapid technological, regulatory, equipment, and security changes demand federal agencies remain flexible and regularly evaluate their communications systems priorities and needs. The result is better agency communications capabilities, but most importantly a reliable and resilient system to operate and respond with during an emergency or critical incident.

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

1. Establish formal emergency communications plans and procedures that guide federal agency deployment of resources and technologies to achieve interoperable communications
2. Federal agencies must use documented formal risk mitigation strategies against physical, cyber-related, response, and attrition risks in emergency communications in order to minimize disruptions to critical communications
3. Explore establishing adequate funding mechanisms to help with lifecycle planning management

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 goals

CORRESPONDING NECP GOAL 3: Develop and deliver training, exercise, and evaluation programs that enhance knowledge and target gaps in all available emergency communications technologies[22]

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

Training, exercises, and evaluation are critical steps to improve emergency communications skills, evaluate capabilities, and assess an organization's progress towards interoperability goals. The COVID-19 pandemic impacted the training and exercise schedules of all federal agencies. Although most in-person engagements were canceled, the virtual exercises held highlighted current and existing limitations due to the lack of in-person emergency communications training, specifically for LMR and communications equipment. As the COVID-19 emergency was sunsetting, most federal agencies were in various stages of transition back to in-person training, with a continued focus on offering hybrid trainings and exercises where appropriate; often driven by cost savings and specific trainings and events which required in-person participation.

Challenges

Shortcomings Remain with Virtual Emergency Communications Training

Over the course of the pandemic, the Federal Government noticed a shift in how it conducted and tracked training and exercises with the transition almost entirely to virtual environments. In 2022, federal agencies noted the most prevalent challenge among federal agencies was the reduction in the number of trainings due to the pandemic. For example, the USA noted the lack of federally sponsored training exercises to practice emergency communications procedures. Large single scale exercises were cut due to funding constraints and there was a focus on virtual

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

training stemming from the pandemic. Federal agencies shared that virtual emergency communication training is perceived as less effective than the comparative in-person trainings. The main critique of the impact to efficacy was noted as a lack of collaboration and networking capabilities, which are a key component of building interoperability and relationships between FSLTT partners. CBP and the Transportation Security Administration (TSA) cited similar gaps in creating realistic scenario-based virtual training to simulate a real-world incident or event that participants would experience while attending an in-person event.

Federal agencies described virtual training as a ‘double-edge sword’; great for reducing costs and increasing access but they limited efficacy and the development of key relationships. While many trainings and exercises were conducted virtually in 2022, many participants explained that some trainings and exercises require in-person instruction and emphasized the benefits of in-person trainings and exercises to bridge gaps in collaboration, coordination, and interoperability. It is recommended that federal agencies strive to re-introduce in-person training, exercises, and other educational engagements to assist in building institutional knowledge and key relationships within the emergency communications community.

Depletion of Emergency Communications Skillsets

Emergency communications personnel often require unique and detailed skillsets. These skillsets are developed and refined through specialized training courses (e.g., Communications Technician [COMT], Communications Unit Leader [COML])[23], on-the-job experience, and documented institutional knowledge. As in-person engagements have become more restrictive due to the COVID-19 pandemic and staff attrition has increased, federal agencies experienced difficulties maintaining emergency communications expertise. Several federal agencies cited significant concerns that the retirement of experienced emergency communications staff could lead to knowledge loss as most qualified staff are nearing retirement age, with many agencies having no plans or contingencies to backfill these positions. Similarly, there are few policy incentives or mechanisms for personnel to advance their careers within the federal emergency communications landscape and there is limited focus on hiring qualified candidates to fill these roles. For example, federal agencies have no set minimum staffing requirements for emergency communications personnel (e.g., COML, COMT) and agencies lack positions for senior emergency communications staff (e.g., COML Type 1).

Federal agencies can take several actions to alleviate these challenges. To ensure optimal level of FSLTT emergency response communications, it is recommended that all partner agencies:

- Continue vendor driven train-the-trainer standardized instruction for procedures and equipment, with demonstrated performance evaluations to enhance incident response;
- Coordinate with federal and SLTT partners to debrief and critique daily operations, mutual aid incidents, and planned events, to address challenges and anticipate gaps in capabilities and resources often not identified during virtual training but through in-person collaboration and calibration efforts; and

[23] Additional information regarding these courses can be found under “Communications Unit Training Resources.” https://www.cisa.gov/safecom/comu-training-resources

- Ensure all partner agencies involved are aware of ongoing funding challenges with training to develop personnel and purchasing equipment or resources critical to a seamless emergency response and incident management.

Successes

Improved Training, Exercises, and Evaluations of Emergency Communications

In 2022, federal agencies continued to prioritize training and exercises that test and evaluate interoperability, infrastructure, cybersecurity, resiliency, and coordination between FSLTT partner agencies. Improved training, exercises, and evaluations of emergency communications were challenged with the continued limitations of COVID-19 and forced agencies to be creative with pathways to learn, develop, and sustain skillsets. The successful outcome and frequency of training, exercises, and evaluations enables federal agencies to provide an optimal level of emergency response, coordination, and communication with SLTT partners.

An example is the USCG's Communications Command and their associated assets who participated in several emergency and incident communications exercises both locally amongst Coast Guard units, and nationally partnering with federal emergency telecommunicators, working through any potential communications hurdles to ensure interoperability is achieved and maintained. In particular, the USCG held four of DHS' virtual COML courses and held its first in-person COMT course since 2019.

Additionally, TSA exercises involved face-to-face interaction as well as on-scene and virtual communication. Other aspects of their exercise communication include planning, response, and after-action report (AAR) phases were included to evaluate all pre-incident, response, and debriefing components. Finally, CBP conducted four hybrid trainings and exercises with the CBP sectors, International Wireless Communications Expo (IWCE), and CBP.

Through improved training, exercises, and evaluations, federal agencies identified key opportunities to leverage aspects of emergency communications when designing future virtual training, in-person mass drills, or tabletop activities. During the 2022 ASA Summit, various agencies highlighted the importance of training, developing rapport with partner agencies, and participating in drills designed to enhance emergency communications, interoperability, coordination, and a successful resolution of an incident.

Emergency Communications Inclusion in AARs Improves

AARs are essential in tracking and documenting performance of emergency communications systems. Most introspective analysis reflects key takeaways, lessons learned, and summarizes observations by all who participated in training, exercises, or major events. Federal agencies, SLTTs, and stakeholders are responsible for following up on AAR recommendations and making the necessary adjustments in policy, procedures, and training to improve emergency communications and ensure limited errors, life safety, and a successful outcome.

In 2022, while the development and tracking of AARs varies widely, several federal agencies identified improvements to this gap in procedures and have taken steps to mitigate and enhance emergency communications by implementing and integrating AARs as part of training and incident debriefs. For example, FirstNet reported that it maintains technical support staff that conducts testing on the ground with users, as well as a team that completes exercise reports and AARs. Further, FirstNet provisions additional resources to assist its users with evaluations such as the Post Incident Event Review (PIER) resource. Also, HHS Assistant Secretary for Preparedness and Response (ASPR) has shared that it continues to include emergency communications performance in AARs and items reported are regularly addressed for corrective actions. Most improvements made to the HHS emergency communications systems are a result of corrective actions derived out of the AAR process (however federal agencies noted that if additional funding is the solution, the problem may not be addressed). Additionally, DHS components have also maintained practices for reporting communications in AARs. USCG held hotwash conversations with communications users to determine best practices, successes, and areas of opportunities for future events and training following communications-related trainings, with recommendations routinely recorded and acted upon shortly thereafter. TSA, through its Intermodal Security Training Exercise System (I-STEP) and Exercise Information Systems (EXIS) programs, developed AARs and documented best practices and lessons learned.

It is critical to continue capturing lessons learned and integrating best practices into emergency communications personnel's roles and responsibilities to ensure optimal response capabilities and resources, as well as indicating any changes to COOP plans and notification processes. The successful outcomes and anecdotal information captured in AARs is critical to improving emergency communications training, exercises, and the federal employee career development process.

COOP and Response Plans Tested Through Trainings and Events

Federal agencies value exercises and training with a focus on testing interoperability, resiliency, coordination, and information sharing to identify gaps and challenges in COOP, SOPs, and cyber incident response plans. It is essential that federal agencies and SLTTs establish policies and SOPs to ensure mission critical functions are maintained during any disruption or threat to routine operations. COOP and cyber incident response plans are developed for planned and unplanned events. The main objectives of these plans are to ensure the safety of personnel, maintain critical mission functions, protect emergency communications equipment, limit disruptions, protect data and its availability, recover quickly, identify alternate sites, and act as a backup Emergency Communications Center (ECC) if necessary.

To guarantee readiness and preparedness of plans, it is recommended that federal agencies leverage training opportunities to evaluate internal federal agency policies and procedures, personnel and communications equipment, succession planning, personnel management, and delegation of authority to better prepare for an actual event. For example, USCG was able to use JAM-X and United Nations General Assembly exercises to evaluate communications outside of normal usage. DOI participated in quarterly joint federal communications testing to determine their ability to communicate under all conditions and to oversee the performance of DOI's essential functions. Further, USDA engaged with its responders to understand how communications equipment was being deployed and which mobile devices are employed in response missions. The information gathered was then used to develop train-the-trainer instruction and activities for use of equipment. The DOE also leveraged exercises to test readiness. For example, DOE participated in Eagle Horizon, hosted in-person tabletop exercises, and partook in the Cyber Storm exercise where DOE trained response procedures in real-time. Additionally, DOE conducted internal testing which included auxiliary testing for reliability, automatic failover testing, providing remote and backup server access, cloud hosting and other cloud-based platforms, and multiple trusted internet connection (TIC) options available for DOE and National Nuclear Security Administration (NNSA) users. Eagle Horizon continues to be a critical event for the Federal Government to evaluate practices and procedures for COOP plans and is an excellent opportunity to determine resource capabilities, systems accessibilities, flexibilities, and resiliency.

Each year, federal agencies are increasingly participating in multi-agency drills to exercise COOP and response plans. These plans were successfully evaluated by simulating real-world events, both planned and unplanned, with growing participation by most federal agencies. Federal agencies evaluated the effectiveness of performing essential functions in the event of emergency communications disruption, evacuation, or unplanned incidents involving natural, man-made, technological, and national security emergencies. It is recommended that federal agencies continue to review and update COOP plans on a routine basis, amending as needed following training and exercises to improve and share response capabilities and points of contact with FSLTT partners.

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

1. Federal agencies should strive to rebuild/re-introduce in-person training, exercises, and other educational engagements to assist in building institutional knowledge and key relationships within the emergency communications community
2. Emergency communications specific job descriptions should be created and modified as needed for public safety staff to enhance retention, specialized training, and career opportunities

Communications Coordination

ASA DEFINITION: Operational processes that enhance interoperable communications during incident response activities

CORRESPONDING NECP GOAL 4: Improve effective coordination of available operable and interoperable public safety communications capabilities for incidents and planned events[24]

OBJECTIVE 4.1: Confirm the implementation of NIMS

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 agencies knowing and sharing information on their emergency communications capacities with partners across all levels of government. Knowledge of available emergency communications assets and resources from partner agencies impacts communications coordination and the ability for federal agencies to respond during critical incidents and planned events. In 2022, the ECPC found federal agencies and their SLTT partners use incompatible equipment and wireless applications during incident response. Also, while collaboration among federal entities is strong, communications coordination preparation for multi-agency response operations varied. Yet agencies continued to improve communications coordination through well maintained COOP (e.g., emergency support function [ESF-2], ESF-7[25]) plans and by exploring communications systems and infrastructure sharing to increase operability and interoperability of emergency communications using fewer resources when responding to incidents and planned events. 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

Equipment and Wireless Application Incompatibility

The ECPC found that incompatibility with communications equipment and other wireless technologies between responders inhibits effective communications coordination. Federal agencies responding to an incident depend on needed communications equipment compatibility for interoperability and enhanced coordination. However, in 2022, federal agencies experienced challenges achieving interoperability during response operations. For example, USDA noted incompatible equipment is a continual challenge during wildland fire response. Partner SLTT

[24] CISA, National Emergency Communications Plan. 2019. cisa.gov/publication/national-emergency-communications-plan.

[25] The Emergency Support Functions (ESF) are explained in the National Response Framework https://www.fema.gov/sites/default/files/2020-04/NRF_FINALApproved_2011028.pdf

agencies often do not have the same encryption or radio capabilities as the federal lead agencies, often forcing responders to use un-encrypted channels.[26] Federal agencies also highlighted challenges with interoperability due to wireless application incompatibility with other FSLTT emergency communications partners using similar applications. The US Coast Guard (USCG) indicated accessing responding partner agencies wireless system applications is difficult as there is no wireless application compatibility standard for wireless application vendors to follow.

As the communications ecosystem and emerging technologies continue to evolve, federal agencies should strive to account for new, improved, or updated capabilities and any challenges that could impact emergency communications systems and coordination across all levels of government. Ensuring communications equipment compatibility and having wireless applications that can interoperate among public safety agencies prior to a joint incident response minimizes communications challenges and improves communications coordination.

Inconsistent Multi-agency Response Operations Preparation Implementation

During large scale critical incidents or planned events proper communications coordination is required to ensure rapid response to an incident. In 2022, federal agencies preparation for multi-agency joint response operations for critical incidents varied. Federal agencies can bolster operational readiness, planning, and communications coordination by taking a proactive approach to learn about SLTT partners communications systems, assets, and resources located within their jurisdiction. In addition, federal agencies should work to formalize the coordination of communications assets and resources with contiguous public safety partners through memoranda of understandings (MOUs) and memoranda of agreements (MOAs) as required. For example, Department of State (DOS) described preparing communications assets for multi-agency response operations on an as needed basis. Additionally, DOS reported not having formal agreements or partnerships in place for joint response efforts. The USA identified steps for preparation of a multi-agency response occurred with local authorities but varied across military bases across the nation. Still agencies like the Federal Protective Service (FPS) prepared for joint operations by purchasing multi-band radios. However, FPS noted the challenge of obtaining MOUs and MOAs for utilization of multi-band radios to operate on the same communications system as the joint response partners.

Effective communications coordination and efficient usage of all available communications capabilities are critical to ensuring both responder safety and the timely provision of public safety services. At a minimum, federal agencies need to share current communications systems information with one another as well as with contiguous SLTT public safety agencies that provide or receive mutual aid, share infrastructure, or participate in joint operations for critical incidents. Sharing active available features, functionality, and capabilities of communications resources with partners expedites communications coordination and renders lifesaving aid to those in crisis.[27]

[26] Additional information regarding technology and infrastructure can be found under "Technology and Infrastructure"

[27] CISA, National Emergency Communications Plan. 2019. cisa.gov/publication/national-emergency-communications-plan.

Successes

Improved Operational Response Readiness

Continuity planning and incident response support the successful execution of critical emergency communication functions and limit disruptions to essential services. Improved operational preparedness and response readiness are results of identifying roles and responsibilities, training, adequate staffing, and preparing personnel to react to planned and unplanned events in support of the continuation of essential functions and coordination with SLTTs towards a timely return to routine operations. While effective communications coordination relies on operational processes, emerging technologies, advanced capabilities, and equipment functionality, utilizing NIMS principles and updated COOP plans significantly benefits incident response, situational awareness, and interoperability.

In 2022, COOP plans, redundancy, and standardized incident response procedures continued to be utilized to maintain mission preparedness and readiness, capable of supporting continued execution of critical agency functions throughout the duration of an event. For example, HHS continued coordination with FEMA's Mobile Emergency Response Support Teams branch through their ESF-8 responsibilities in response to COVID-19. TREAS followed NIMS principles and updated their COOP plan with periodic testing of their Radio-Over-IP (RoIP) system every quarter. GSA assesses the readiness of their organization's emergency communications systems and personnel by evaluating their communications capabilities annually, monthly, and conduct daily internal communications testing.

The FCC has a COOP plan which addresses continuity training and continuously updates the curriculum and details roles and responsibilities for the FCC's relocation and devolution response groups. The FCC ensures the plans are updated on an annual requirement by midyear in preparation for Eagle Horizon. DOI headquarters and continuity elements participate in a joint federal communication quarterly testing used to determine DOI's ability to communicate under all conditions and to oversee the performance of DOI's essential functions. DOJ noted their readiness assessment of emergency communications systems and personnel for day-to-day operations and out-of-the-ordinary incidents are coordinated by the component headquarters and field divisions. DOE improved cross-site intergovernmental collaboration through investments in cloud-based technologies services for unclassified and classified systems across the enterprise, increased classified redundancy, and mission flexibility while maintaining a secure data protection capability, and meeting data center requirements to ensure NNSA data and information.

Despite COVID-19 and the inability to integrate some training and exercises across enterprises, federal agencies were successful in conducting their missions by utilizing robust COOP plans and following NIMS principles for incident response. It is recommended that testing continues on an annual basis or with more frequency to ensure all mission essential functions are carried out by agencies and SLTTs in the event of a threat or emergency. Agencies should continue to maintain mission readiness and identify opportunities for improvement. As well, agencies should develop effective scenario-based training which ensures successful resolution of emergency incidents and reinforces institutional knowledge that can be leveraged for future events. Applying best practices and lessons learned to evaluate agencies' incident response plan capabilities, prioritizes effective communications coordination, and execution of response ready mission critical functions.

Collaborative Coordination and Interagency Resource Sharing with SLTT Partners

Achieving a strong, reliable, and resilient communications system for effective communications coordination requires federal agencies to leverage and seek out all available communications assets and resources across the different levels of government. As depicted in Figure 1, communications systems and infrastructure sharing includes various aspects of communications such as the assets—physical infrastructure (e.g., tower sites, facilities, repeaters, connectivity), real estate, spectrum, applications, subscriber units, and technical and operational or staff—contributed in support of these critical communications. Once established, these systems may expand to include other technologies, capabilities, and subscribers across all levels of government, enhancing operability, interoperability, resiliency, and security.[28]

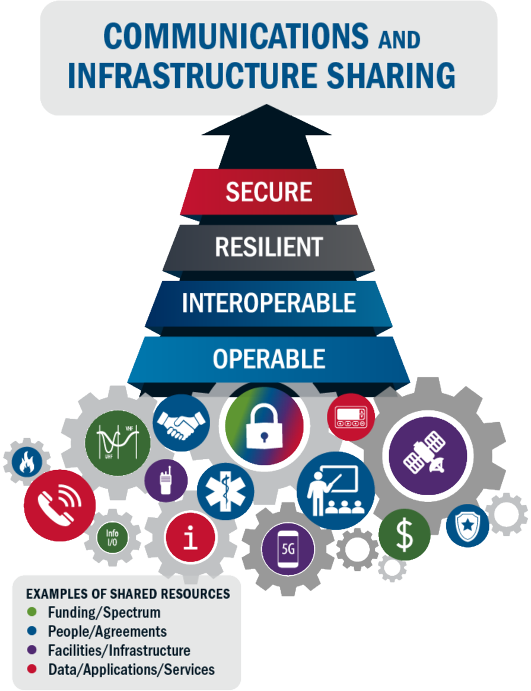
COMMUNICATIONS AND INFRASTRUCTURE SHARING
SECURE
RESILIENT
INTEROPERABLE
OPERABLE
Info I/O
5G
$
EXAMPLES OF SHARED RESOURCES
● Funding/Spectrum
● People/Agreements
● Facilities/Infrastructure
● Data/Applications/Services

Figure 1: Communications and Infrastructure Sharing Overview

In 2022, federal agencies engaged FSLTT partners to share communications systems and infrastructure which lead to improved communications coordination and interoperability. For example, DoD shared that the National Guard (NG) has LMR agreements with Alaska and other states. The federal government and states share repeater systems; other states have similar systems with their NG coordinating with state response services. The DOJ law enforcement (LE) components shared LMR infrastructure with each other and other federal partners and states as needed. In a non-traditional sense, the FCC shares sensor equipment with FSLTT partners for situational awareness to better understand their current public safety operating environment. Data from these shared sensors informs the operations and actions of mutual aid partners and raises the situational awareness of all with access. Finally, FPS, CBP, and FLETC reported sharing systems by utilizing the ICE core[29] for their communications networks.

In 2022, the ECPC established the Federal Resource Sharing Working Group. This group's goal is to explore how federal agencies can leverage system sharing to increase operability and interoperability. The Working Group is focused on developing documentation to inform federal

[28] Cybersecurity and Infrastructure Security Agency "SCSI Along the Southwest Border," December 2019.
[29] The core is the primary controlling source of a land mobile radio system, responsible for servicing and supplying serviceability to its features, functions, and attached fixed network infrastructure through connectivity.

agency decision makers and explain the importance of shared communications and infrastructure initiatives. As 2022 came to a close, the Work Stream was finalizing their first set of documents:

- The Proposed Evolution of Federal Public Safety Communications; Volume 1: Land Mobile Radio Systems
- Funding and Sustaining Federally Shared Land Mobile Radio Systems

Federal agencies should continue to seek opportunities to share communications systems and infrastructure by developing a culture of supporting shared systems within the Federal Government and working to lower barriers to implementing shared systems for effective communications coordination.

LOOKING AHEAD:
Communications Coordination Recommendations for Federal Departments and Agencies

1. Continue to encourage the use of NIMS compliant assets across the federal interagency landscape
2. Discover collaborative partnerships for shared emergency communications services that address roles, responsibilities, liabilities, spectrum, infrastructure, data interoperability, cybersecurity, and data sharing needs

Technology and Infrastructure

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

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[30]

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 2022, federal partners identified challenges in the acquisition and maintenance of emergency communications systems, as well as success in deploying novel communications technologies to improve interoperability.

[30] CISA, National Emergency Communications Plan. 2019. cisa.gov/publication/national-emergency-communications-plan.

Challenges and Priorities

Federal Agencies Rely on Commercial-Off-The-Shelf (COTS) Equipment To Support Emergency Communications Missions

In 2022, federal agencies reported using a variety of COTS emergency communications systems to complete their public safety, disaster response, and emergency communications missions; however, recent supply chain shortages have highlighted an over-reliance in the emergency communications community. COTS systems are often the most cost effective, robust, and efficient way to support federal emergency communications missions. For example, the FirstNet device ecosystem (which a majority of federal agencies utilize) consists of an extensive range of COTS devices (to include smartphones, tablets, routers, modems, and wearables). These devices support push-to-talk capabilities and bridge gaps to enable interoperability between LMR and wireless broadband networks.

TREAS noted that the COTS systems they employ enable interoperability with other FSLTT personnel, as they often use the same systems. However, even with these benefits, the federal emergency communications community identified an often over-reliance on COTS systems. As a result of pandemic related supply chain disruptions, several agencies explained that they were unable to procure mission critical systems or follow lifecycle plans in the replacement of end-of-life systems. The failure to replace old and end-of-life equipment places the emergency communications community at increased risks of system failures and cyber-threats (as these systems no longer receiving security patches and updates).

Additionally, suppliers/vendors for specialized emergency communications equipment are limited (often there are only up to two vendors providing these emergency communications specific systems). This limitation exposes the Federal Government and its public safety partners to a greater risk of supply chain attacks.[31]

While it is not feasible for the Federal Government to develop their own emergency communications systems or mitigate these threats completely, federal agencies should evaluate and understand the risks to their emergency communications supply chain and build plans to ensure security and equipment lifecycles can be maintained.

Roadblocks Persist in The Implementation of Electric Vehicles into Public Safety and Emergency Communications Missions

As a continuation of efforts from 2021, several federal agencies are re-aligning acquisitions processes to focus on the procurement of electric vehicles (EV) in their transportation fleets as outlined in Executive Order 14057 *Catalyzing Clean Energy Industries and Jobs Through Federal Sustainability*[32]. While the federal emergency communications community has recognized the need to transition to EVs, federal agencies have varying experiences when installing standard emergency communications equipment. For example, in 2022 the Federal

[31] Supply chain attacks are cyber-attacks that seek to damage or otherwise compromise an organization by targeting upstream supply chain elements

[32] E.O. 14057: Catalyzing Clean Energy Industries and jobs Through Federal Sustainability. fedcenter.gov/programs/eo14057/

Protective Service (FPS) experienced success in deploying their fully electric law enforcement vehicle.[33] However, other federal agencies have not shared this success. For example, several agencies noted that they have continued to find incompatibilities between EVs and standard emergency communications electronics. Federal agencies are working to identify mitigations however, the current identified solutions require the purchase of additional equipment or adapters that are not approved for federal use.

Additionally, federal agencies have identified several problems in their functionalities and support infrastructure. For example, departments such as DOI, USDA, and DOL (specifically the Mine Safety and Health Administration [MSHA]) often operate in rural locations which lack EV charging infrastructure. Further, few EVs are available that could meet the driving conditions needed to support emergency communications and response in remote areas.

To speed up and improve the implementation of EVs for federal emergency communications users, federal agencies should collaborate in the development of technology standards and a technology roadmap to streamline the transition from internal combustion vehicles to ensure that emergency communications technology remains operable in EVs. Until the Federal Government addresses the challenges with range, absence of charging infrastructure, and logistical challenges (i.e., charging during disaster response), EVs will not be ideal to support mission critical and emergency response operations.

Successes

Innovative Technologies Enhance Federal Emergency Communications

Federal agencies are continuously looking for new and enhanced technologies that will support their emergency communications systems. In 2022, agencies were able to pilot and implement several innovative technologies for emergency communications uses. The NPSBN was the most utilized emerging technology in 2022, with TREAS, USDA, DOI, DoD, and DOJ all reporting either piloting or using it to supplement mission critical public safety communications and enhance interoperability with partners.[34] Notably, federal agencies leveraged NPSBN capabilities to deploy satellite cell on a light truck (SatCOLT) as well as compact rapid deployables (CRDs) in response to Hurricane Ian. In addition, USDA collaborated with the National Aeronautics and Space Administration (NASA) to investigate the feasibility of deploying telecommunications equipment on high altitude balloons over incidents to provide better coverage in difficult terrain. Currently USDA is investigating whether or not the use of existing high-altitude equipment can be NPSBN certified and if existing NPSBN equipment can operate at high altitudes.

With the added connectivity capability that NPSBN provides, federal emergency communicators increasingly leveraged cloud-based services. Cloud services have proven useful to enhance collaboration, improve coordination, and enhance redundancy. For example, DOE's ESF-2

[33] DHS, DHS Electric Vehicle Program Accelerates with Debut of First Fully Electric Law Enforcement Vehicle. 2022. Dhs.gov/news/2022/09/19/dhs-electric-vehicle-program-accelerates-debut-first-fully-electric-law-enforcement

[34] Federal agencies did note that even with the increasing deployment, coverage, and capabilities of PSBN, it is not to be considered a replacement of traditional LMR communications networks.

Support Team has expanded the use of Microsoft Teams, creating a focused channel on incidents so that all documents and communications are centrally located. DOE was previously reliant on email and cell phones. DOE has also established a continuity portal for central records management (CRM). This portal ensures that essential records are available at all times. DOS has further leveraged cloud-based services in the implementation of their Web Emergency Operations Center (WebEOC). The WebEOC platform provides a resilient platform for DOS' worldwide emergency management needs.

Finally, federal agencies are also enhancing legacy communications systems to improve their capabilities and reliability. For example, TREAS is installing radio gateways for its RoIP systems. These gateways will connect local radio communications with cell phones, enhancing interoperability.

To ensure that agencies are remaining vigilant and taking advantage of beneficial emerging technologies, federal emergency communication staff should continue to maintain awareness of the progression of industry technology and work to lower administrative barriers to pilot and incorporate new technologies.

Federal Agencies Continue to Transition to NG911; However Work Remains

Federal agencies have been slowly working to implement the suite of technologies that compose NG911 while there has been significant progress in lowering hurdles to further NG911 implementation. For example, DoD, the largest federal entity that is managing a transition to NG911 systems, has established the BECS Program[35] which ensures funding for emergency communications improvements into the future. The BECS program will act as the single integrated acquisitions program for the design, procurement, fielding, new equipment training and life-cycle management of emergency management/critical communications capabilities in support of installation public safety organizations and functions, including first responder, force protection and other installation management activities. This program is expected to greatly assist the DoD in their implementation of NG911 systems at installations nationwide. Also, DoD has implemented a mandate to move away from time-division multiplexing (TDM) by 2025.

Other agencies have taken steps to reduce barriers to NG911 adoption for other federal partners. For example, the DHS Science and Technology Directorate (S&T) is conducting research and development activities to utilize NIST cybersecurity assessment of NG911 technical architecture and conduct assessments of the cybersecurity posture of Public Safety Answering Points (PSAPs). S&T is conducting pilots of the proposed solution that will enable PSAPs to assess and document their cyber hygiene and aid in the development of plans and actions along with reporting and documentation. The DOC also reported the use of the NPSBN as a third layer for resiliency/redundancy backhaul for public safety working to transition to NG911. These supporting programs will further reduce the barriers that federal agencies experience when deploying NG911 systems.

[35] The BECS program encompasses capabilities that will deliver computer-aided dispatch (CAD), NG911, LMR, enterprise mass warning and notification (EMWN), and public safety broadband networks (PSBN).

However, with all these efforts, there are still challenges that federal agencies face in the implementation of NG911. For example, federal agencies noted that the federal government needs to recognize the importance of geospatial data in the implementation of NG911. NG911 implementation requires every locality to be accurately mapped to support dispatching. There is currently no federal capability to support collection of this data due to limited resources. Mapping efforts often take several months and include making sure that building addresses and signs are accurate. Federal agencies are facing continued challenges in the prioritization of NG911 resources in budget planning, often relying on unallocated funds to implement 911 system updates.

In order to ensure the continued implementation of NG911, federal agencies should establish dedicated lines of funding, similar to the BECS program, to support the maintenance and modernization of emergency communications and public safety communications systems.

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

1. Evaluate the risks in emergency communications supply chains and build plans to ensure that federal agencies equipment lifecycles can be maintained
2. Develop federal standards or a roadmap for the integration of EVs in mission critical, emergency communications, and public safety transportation fleets to streamline the transition from internal combustion vehicles
3. Establish dedicated lines of funding to support the maintenance and modernizations of federal emergency communications systems

Cybersecurity

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

CORRESPONDING NECP GOAL 6: Strengthen the cybersecurity posture of the Emergency Communications Ecosystem[36]

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

Each federal agency has a responsibility to keep their networks secure, including computer networks, websites, as well as emergency communications tools and equipment. In 2022, the

[36] CISA, National Emergency Communications Plan. 2019. cisa.gov/publication/national-emergency-communications-plan.

Federal Government largely succeeded in keeping systems secure and operable throughout steady-state and incident response operations. However, as new security standards and technologies are implemented, federal agencies are finding challenges with the integration of emergency communications systems, as these systems often have unique operational requirements.

Challenges and Priorities

System Availability is the Dominant Cybersecurity Concern for Emergency Communications

As the Federal Government incorporates new technologies into their emergency communications operations, existing systems are exposed to the Internet Protocol (IP) threat environment. These threats target the confidentiality[37], integrity[38], and availability[39] of networks. In 2022, federal agencies uniformly reported that their primary cybersecurity concern was the availability of secure emergency communications systems. Maintaining communications availability through working networks is a particular challenge as there are several advanced and persistent threats which could impact emergency communications, such as:

- Distributed Denial of Service (DDoS) Attack: occurs when multiple machines are operating together to attack one target[40]
- Ransomware Attack: a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption[41]
- Electromagnetic Pulses (EMP): a burst of electromagnetic energy with the potential to negatively affect technology systems on Earth and in space[42]
- Communication line cuts/outages: either malicious or accidental, damage to physical communications lines stop or hinder communications until repairs or alternate routings can be made.[43] This is a particular challenge as federal agencies are largely dependent on commercial communications networks[44]

[37] Confidentiality refers to the capability of networks to protect sensitive data from unauthorized release or access

[38] Integrity refers to the capability to ensure data is not modified or deleted by unauthorized or malicious actors

[39] Availability refers to the capability to ensure that systems and data are available to users when needed and under any circumstances

[40] CISA, Understanding Denial of Service Attacks. https://www.cisa.gov/news-events/news/understanding-denial-service-attacks

[41] CISA, Stop Ransomware. https://www.cisa.gov/stopransomware

[42] White House, Executive Order on Coordinating National Resilience to Electromagnetic Pulses. https://www.federalregister.gov/documents/2019/03/29/2019-06325/coordinating-national-resilience-to-electromagnetic-pulses

[43] CISA, Public Safety Communications Resiliency, Ten Keys to Obtaining a Resilient Local Access Network. https://www.cisa.gov/sites/default/files/publications/07202017_10_Keys_to_Public_Safety_Network_Resiliency_010418_FINAL508C.pdf

[44] FSLTT departments and agencies can find additional information regarding communications dependencies on commercial infrastructure in CISA's Public Safety Communications Dependencies on Non-Agency Infrastructure and Services.

Federal agencies must continue to invest in technology, processes, and people to mitigate these challenges. In order to maintain a strong and resilient IT and emergency communications environment, federal agencies must continue to research, deploy, and appropriately resource emergency communications resiliency measures to ensure the operability and connectivity of mission critical communications systems.

Uneven Implementation of the Advanced Encryption Standard (AES) Hinders Security and Interoperability

Encryption of LMR communications has increasingly been a standard practice to protect the confidentiality of data in emergency communications systems. Federal agencies have been mandated to transition from the data encryption standard (DES) to AES and may not use older standards. However, SLTT partners are often still in the process of moving to the AES standards or maintain LMR systems that are not capable of supporting any encryption standard. In 2022, federal agencies highlighted several challenges caused by this disparity between federal and SLTT adoption of encryption standards. For example, in wildland fire response, USDA-United States Forest Service (USFS) often is forced to operate unencrypted radios as their SLTT partners in areas of response do not have encryption capabilities. As a result, in 2022, USDA-USFS experienced multiple examples of radio interruptions during wildland fire responses where unknown users accessed emergency communications LMR channels to redirect firefighting resources. USDA-USFS' only recourse to combat this issue was to notify the FCC and law enforcement (and in these cases, FCC and law enforcement personnel were unable to locate the offenders). DOI also noted difficulty maintaining interoperability with SLTT partners as a result of differing encryption standards. DOI also shared that it expects these interoperability challenges to continue as the resolutions are largely out of federal control. This challenge highlights that federal agencies accustomed to operating with encryption are put at an interoperability disadvantage and can struggle to pivot when there is need to communicate on non-encrypted channels.

There are several mitigation efforts that federal agencies can undertake to help resolve this challenge. Federal agencies should continue to maintain communications caches (hand-held radios) or arrange sharing agreements. These caches ensure that federal responders are all able to use the compatible communications equipment during a joint response. Federal agencies can also work to identify SLTT partners in need of assistance in migration to AES and direct them to the appropriate resources, grants, and other technical assistance in order to speed the acceptance of digital LMR and AES.

Successes

Emergency Communications Systems were Unimpacted by Cybersecurity Incidents in 2022 Due to Robust Security and Response Plans

Federal emergency communications networks are a prime target for cyber disruptions by malicious actors and face constant cybersecurity threats. Despite these constant attacks and threats, in 2022, Federal Civilian Executive Branch (FCEB) agencies were able to maintain the integrity and security of emergency communications networks. Two key practices helped protect federal networks, the utilization of National Institute of Standards and Technology (NIST) cybersecurity framework and broad cybersecurity information sharing. The NIST cybersecurity framework provides guidelines for securing networks to reduce and manage cyber risks. The NIST cybersecurity framework is also intended to "foster risk and cybersecurity management communications amongst both internal and external organizational stakeholders."[45] Per E.O. 13800 *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*[46], FCEB agencies and federal contractors are required to apply the framework to their networks. All federal agencies continued to report the application of the NIST cybersecurity framework in 2022.

Federal agencies also continued to report participating in comprehensive two-way information sharing with CISA. Cybersecurity information sharing across federal agencies enables actionable, relevant, and timely information exchange to help detect, prevent, mitigate, and ultimately respond to cybersecurity threats. For example, in 2022, DOI reported leveraging its Cyber Intelligence Group to share threat information to FSLTT partners via email, threat exchange partner calls, and in-person through the DOI liaison within the FBI National Cyber Investigative Joint Task Force Office. GSA also noted participating in extensive cybersecurity information sharing activities. In 2022, GSA noted leveraging the formal mechanisms, such as sharing threat information with CISA, when malicious files or cyberattacks were encountered. GSA also utilized the Homeland Security Information Network (HSIN) portal as well as Cyber Liaisons.

Federal agencies have developed cybersecurity incident response plans in the event that a vulnerability is found in emergency communications systems. These plans outline instructions and personnel roles to help detect, respond to, and recover from cyberattacks, service outages, or other cyber-related incidents. For example, in 2022, the FCC completed the development of their Cyber Incident Response Playbook. This playbook was developed in accordance with the CISA Federal Government Cybersecurity and Incident Response Playbooks.[47] Several other agencies also maintained their cyber response plans in 2022. For example, the DOE maintains their All-Hazards Response Plan, which contains an annex which addresses cyber incident response. The DOE is also in the process of developing a Cyber Incident Response Strategy to outline how the department can assist the energy sector in their cyber incident responses (i.e., to assist in mitigations from attacks such as the Colonial Pipeline hack). DOS also noted that they maintained a Cybersecurity Incident Response Team (CIRT) that is responsible for detecting, responding to, and managing all cyber incidents that impact DOS networks. The DOS CIRT has well established plans, policies, and operational procedures for providing detail response on specific incidents and working closely with system owners and Information System Security Officers to fully mitigate threats and vulnerabilities stemming from cybersecurity threats.

While federal emergency communications are under robust cybersecurity protections, there are opportunities to make updates to policies and procedures to allow for greater protection and functionality specific to emergency communications systems. Federal agencies identified two

[45] NIST, Framework for Improving Critical Infrastructure. 2018. Nist.gov/cyberframework

[46] E.O. 13800 Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. 2017. federalregister.gov/documents/2017/07/12/2017-14553/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure-workforce

[47] CISA, Federal Government Cybersecurity Incident & Vulnerability Response Playbooks. November 2021. https://www.cisa.gov/sites/default/files/2023-02/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf

cybersecurity configurations hindering emergency communications operations. For example, DOI reported the issue of not being able to use “Dual Homing[48]” networked PCs due to security standards. DOI noted this functionality would be ideal for interagency dispatch centers with many networks. DOI added that currently it is authorized, but controls are too strict to enable the feature. TREAS reported that Federal Information Security Modernization Act (FISMA) controls are challenging to implement for LMR and RoIP systems.

To ensure that emergency communications remain unimpacted by cybersecurity incidents, federal agencies should continue to follow cybersecurity standards and investigate how to include all emergency communications needs and functionalities fit into cybersecurity best practices.

Greater Focus on Implementation of Zero Trust Architecture (ZTA)

In accordance with E.O. 14028 *Improving the Nation’s Cybersecurity*[49], FCEB agencies are working to implement ZTA. ZTA assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (e.g., local area networks versus the internet) or based on the asset ownership (e.g., enterprise provisioned or personally owned). Authentication and authorization (both subject and device) are discrete functions performed before a session when a resource is established. ZTA is a response to enterprise network trends that include remote users, bring your own device (BYOD), and cloud-based assets that are not located within an enterprise-owned network boundary. ZTA focuses on protecting resources (e.g., assets, services, workflows, network accounts), not network segments, as the network location is no longer seen as the prime component to the security posture of the resource.[50] Since 2021, agencies have made significant progress towards hardening their emergency communications and internal networks with these policies. For example, both USDA and DOI reported developing long-term plans for implementation of ZTA, identifying requirements gaps, and setting implementation timelines in accordance with administration goals. Some agencies are more mature in their implementation of ZTA in their communications networks. For example, in 2022, GSA reported that they are in year two of their ZTA implementation plan and are approximately 70 percent complete. GSA noted that they are ahead of the Office of Management and Budget (OMB) Enterprise Architecture Memorandum 22-09[51] requirements and have moved security to a secure access edge solution for GSA via virtual private networks (VPN) and GSA facilities. GSA also plans to continue implementing micro-segmentation for users and devices for operational technology internet of things (IOT) across the 500 buildings that they manage (as of April 2022, approximately 200 buildings have been completed).

Even with these achievements there are some federal agencies still facing challenges in implementing ZTA that are specific to emergency communications. One of the most significant

[48] Dual Homed devices refer to a device that is connected to more than one network interface for redundancy, interoperability, or security purposes

[49] E.O. Improving the Nation’s Cybersecurity. 2021. federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

[50] NIST, NIST SP 800-207, Zero Trust Architecture | NIST

[51] EOP, Enterprise Architecture Memorandum 22-09 Moving the U.S. Government Towards Zero Trust Cybersecurity Principles. January 26, 2022. https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

challenges is the integration of LMR systems into ZTA. For example, multi-factor authentication (MFA) is a key tenet of ZTA and LMR handsets are not capable of integrating this feature. This alone presents a challenge towards implementation of ZTA in emergency communications as LMR remains the industry standard for public safety and emergency communications system.

As federal agencies continue to deploy ZTA in their emergency communications networks, they should communicate, develop, and share best practices to speed implementation and solve shared challenges.

LOOKING AHEAD:
Cybersecurity Recommendations for Federal Departments and Agencies

1. The federal emergency communications community should work to identify SLTT partners in need of assistance in migration to AES encryption and direct them to the appropriate resources, grants, and other technical assistance
2. Agencies should continue to research and deploy resiliency measures to ensure operability and connectivity of mission critical communications systems
3. As federal agencies continue to deploy zero-trust architectures in their emergency communications networks, they should communicate, develop, and share best practices to speed implementation and solve shared challenges
4. Federal agencies should continue to follow set cybersecurity standards and investigate how to ensure all emergency communications needs fit into cybersecurity best practices

V. Conclusion

In 2022, federal agencies coordinated across all levels of government to provide an update on the status of public safety communications capabilities in support of emergency response operations. Using the NECP as a roadmap, federal partners worked towards increasing interagency and national emergency communications capabilities. Federal partners demonstrated progress towards achieving the NECP goals and reported challenges to increased interoperability, including:

- Enhancing governance structures by incorporating non-traditional stakeholders e.g., IT personnel to expand the communications decision-making process, maintaining strong interagency relationships, and sustaining administrative processes that prioritize communications needs;
- Identifying resources to facilitate the adoption of a FIC and highlighting methods to enhance communications governance maturity;
- Exercising regular review and update sessions for communications plans and conducting communications needs evaluation to improve interoperability;
- Incorporating lifecycle planning and exploring formal risk mitigation strategies to strengthen emergency communications;
- Continuing to improve training, exercises, and evaluations of emergency communications by including communications in the AAR process, and testing COOP and response plans through training events;
- Assessing the impact of the virtual communications training environment and identifying solutions to mitigate the loss of specialized communications knowledge and experience in the Federal Government due to attrition;
- Demonstrating improved communications response readiness through collaborative coordination and resource sharing with SLTT;
- Focusing on improving communications security gaps and utilizing emerging technologies to enhance emergency communications operability;
- Deploying emerging technologies to support federal emergency communications systems and continuing with the transition to NG911; and
- Maintaining robust security and response plans as federal agencies continue to implement ZTA.

Moving forward, the 2022 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 these findings in their strategic planning processes. Through this effort, 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 emergency events.

VI. Appendices

Appendix A: Abbreviations/Definitions

AAR	After Action Report
AES	Advanced Encryption Standard
ASA	Annual Strategic Assessment
ASPR	Assistant Secretary for Preparedness and Response
BECS	Base Emergency Communications System
BLM	Bureau of Land Management
BYOD	Bring your own device
CBP	Customs and Border Protection
CDC	Center for Disease Control and Prevention
CIO	Chief Information Officer
CIRT	Cybersecurity Incident Response Team
CISA	Cybersecurity and Infrastructure Security Agency
COML	Communications Unit Leader
COMT	Communications Technician
COOP	Continuity of Operations
COTS	Commercial Off-the-Shelf
COVID-19	Coronavirus Disease of 2019
CRD	Compact Rapid Deployables
CRM	Central Records Management
DCIO	Deputy Chief Information Officer
DDoS	Distributed Denial of Service
DEA	Drug Enforcement Administration
DES	Data Encryption Standard
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DOE	Department of Energy
DOI	Department of the Interior
DOJ	Department of Justice
DOL	Department of Labor
DOS	Department of State
DOT	Department of Transportation
ECPC	Emergency Communications Preparedness Center

EMB	Enterprise Management Board
EMP	Electro Magnetic Pulse
EV	Electric Vehicle
EXIS	Exercise Information System
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FCEB	Federal Civilian Executive Branch
FCIELT	Field Communications Improvement Executive Leadership Team
FEMA	Federal Emergency Management Agency
FIC	Federal Interoperability Coordinator
FirstNet	First Responder Network Authority
FISMA	Federal Information Security Modernization Act
FLETC	Federal Law Enforcement Training Centers
FMR	Federal Mission Resilience
FPS	Federal Protective Service
FSLTT	Federal, State, Local, Tribal, and Territorial
FTA	Federal Transit Administration
GSA	General Services Administration
HHS	Department of Health and Human Services
HSPD	Homeland Security Presidential Directive
IOT	Internet of Things
IP	Internet Protocol
IPAWS	Integrated Public Alert and Warning System
I-STEP	Intermodal Security Training Exercise Program
IT	Information Technology
ITAB	Information Technology Governance Board
IWCE	International Wireless Communications Expo
JAM-X	Jamming Exercise
JRIMS	Joint Requirements Integration and Management System
JWPMO	Joint Wireless Program Management Office
LE	Law Enforcement
LMR	Land Mobile Radio
LPG	Legacy Public Safety Gateways
MFA	Multi-Factor Authentication
MSHA	Mine Safety and Health Administration

NASA	National Aeronautics and Space Administration
NCP	National Continuity Policy
NECP	National Emergency Communications Plan
NNSA	National Nuclear Security Administration
NIFOG	National Interoperability Field Operational Guide
NIMS	National Incident Management System
NIST	National Institute of Standards and Technology
NPSBN	Nationwide Public Safety Broadband Network
NTIA	National Telecommunications and Information Administration
OCIO	Office of the Chief Information Officer
OEMD	Operations and Emergency Management Division
OGA	Other Government Agencies
OMB	Office of Management and Budget
PIER	Post Incident Event Review
PSAPs	Public Safety Answering Points
RoIP	Radio Over Internet Protocol
S&T	Science and Technology
SatColt	Satellite Cell on a Light Truck
SCSI	Shared Communications Systems and Infrastructure
SLTT	State, Local, Tribal, and Territorial
SOP	Standard Operating Procedure
SOTU	State of the Union
TDM	Time Division Multiplexing
TIC	Trusted Internet Connections
TIGTA	Treasury Inspector General for Tax Administration
TREAS	Department of the Treasury
TSA	Transportation Security Administration
TWG	Technology Working Group
UNGA	United Nations General Assembly
USA	United States Army
USC	United States Code
USCG	United States Coast Guard
VPN	Virtual Private Network
WCB	Wireless Control Board
WebEOC	Web Emergency Operations Center

ZTA	Zero Trust Architecture

Appendix B: Interview Participants

DEPARTMENT OR AGENCY	COMPONENT
Department of Commerce	• First Responder Network Authority • National Institute of Standards and Technology (NIST) Public Safety Communications Research Division • National Telecommunications and Information Administration (NTIA) Office of International Affairs • NTIA Office of Policy Analysis and Development • NTIA Office of Public Safety Communications • NTIA Office of Spectrum Management
Department of Defense	• Deputy Chief Information Officer Command, Control, Communications Infrastructure (C3I) • Defense Information Systems Agency • Marine Corps Installations Command (G-3) • Marine Corps Installations Command (G-6) • Office of the Chief Information Officer • U.S. Army • U.S. Marine Corps • U.S. Navy
Department of Health and Human Services	• Office of the Assistant Secretary for Administration • Office of the Assistant Secretary for Preparedness and Response • Office of the Chief Information Officer • Office of Incident Command and Control • Office of Resource Management
Department of Homeland Security	• Customs and Border Protection • Federal Emergency Management Agency • Federal Law Enforcement Training Centers • Federal Protective Service • U.S. Immigration and Customs Enforcement • Joint Wireless Program Management Office • Transportation Security Administration • U.S. Coast Guard • U.S. Secret Service
Department of the Interior	• Office of the Chief Information Officer • Office of Wildland Fire
Department of Justice	• Justice Management Division • Federal Bureau of Prisons
Department of Labor	• Mine Safety and Health Administration

DEPARTMENT OR AGENCY	COMPONENT
Department of State	• Bureau of Diplomatic Security • Bureau of Information Resource Management • Diplomatic Continuity Programs • Operations Center
Department of Transportation	• Federal Aviation Administration • Federal Highway Administration • National 911 Program • Office of the Chief Information Officer • Office of Intelligence, Security, and Emergency Response • U.S. Maritime Administration
Department of the Treasury	• Internal Revenue Service Criminal Investigation • Treasury Inspector General for Tax Administration
Federal Communications Commission	• Office of the Chief Information Officer • Public Safety and Homeland Security Bureau
General Services Administration	• GSA IT • Office of Mission Assurance

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. 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?
    a. Is your department/agency participating in or leading any new groups or initiatives?
2. 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/agency performed threat assessments or resource prioritization?
    b. What is your department/agency's current emergency communications priorities?
3. How does your department/agency balance sustainment of existing communications technologies with building new communications capabilities?
4. How can the Emergency Communications Preparedness Center (ECPC) better assist federal organizations implement new or enhance interoperability communications?
5. Does your department/agency have a plan to implement a Federal Interoperability Coordinator or otherwise designate a lead division to manage emergency communications interoperability?

Planning and Procedures

1. What documentation does your department/agency use to outline emergency communications goals, strategies, and timelines?
    a. If your department/agency made updates, how did the review or updates occur? What factors influenced your decision? What impacts on communications capabilities does your department/agency anticipate from the changes?
        i. How frequently does your department/agency measure progress towards its strategic plan or success indicators?
    b. If your department/agency has not made updates, how did your department/agency assess your current strategic plan to ensure it met your workforce's needs?
2. In 2022, has your department/agency identified any communications capability gaps?

Do you plan to address these gaps in your strategic plan?

   a. If yes, what steps has your department/agency taken to address these concerns? Were these gaps addressed in your strategic plan?

3. What types of risk management strategies (e.g., communications assessments, training, testing, or exercises, incident response strategy) does your department/agency incorporate into plans for continuity and recovery of communications systems?

Training, Exercises, and Evaluation

1. In 2022, did your department/agency continue to utilize virtual environments for training and exercise events or was there a return to in-person activities?
   a. What influenced your department/agency's decision and how has it impacted communications capabilities?
2. In 2022, how many communications focused exercises (e.g., in-person or virtual tabletop) did your department/agency participate in?
   a. If yes, 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. If no, how did your department/agency test communications readiness without exercises? How does your department/agency incorporate lessons learned or after-action report findings?
3. In 2022, did your department/agency identify any technical or operational capability gaps as a result of training/exercise engagements?
   a. If yes, what actions did your department/agency take to close capability gap(s)?
   b. If no, how does your department/agency evaluate communications capabilities during training and exercises?
4. When fielding new communications equipment, how does your organization update training and exercise programs? How is this training conducted (e.g., train-the-trainer)?
5. 5. Does your department/agency formally evaluate (e.g., after-action report, action summary report, etc.) training exercises and document lessons learned?
   a. If yes, how does your department/agency track against the progress identified communications gaps?
   b. If no, how are challenges identified and remediated?
6. In 2022, how did your department/agency assess the readiness of its communications systems and personnel both day-to-day and out-of-the-ordinary situations?
7. In 2021, several agencies reported inconsistent inclusion of emergency communications performance in After Action Reports (AAR). How frequently is the performance of emergency communications included in AARs in 2022?

   a. What are some of the challenges or reasons for not including communications in AARs?

Communications Coordination

1. Federal departments and agencies have widely standardized National Incident Management System (NIMS) for incident response. How has NIMS trainings/resource typing impacted your department or agency's communications capabilities?
   a. Does your department/agency utilize another standard for training or resource typing?
   b. Are there any challenges or recommended improvements for NIMS you would like to share?
2. In 2022, how many times did your department/agency partner with other Federal, State, Local, Tribal, and Territorial (FSLTT) partners during response operations?
   a. Did your department/agency identify any communications-related operational challenges during joint response operations (e.g., spectrum management, broadband capacity, incompatible equipment, lost or damaged communications infrastructure, inconsistent access to power supplies)?
   b. How does your department/agency prepare communications assets for multi-agency jurisdictional response operations?
   c. Has the use of the Advanced Encryption Standard (AES)-encrypted radio resources helped or hindered your agency's ability to communicate with other FSLTT agencies?
3. In 2022, how did your department/agency ensure continuity of communication during response operations?
   a. Did your department/agency encounter any challenges maintaining reliable/interoperable communications?
   b. If yes, how did your department/agency close that capability gap?
4. In 2022, did your department/agency establish new or update any existing formal written agreements with FSLTT entities that define roles and responsibilities during response operations (e.g., memoranda of understanding/agreement, inter-agency agreements)?
   a. If yes, with whom do you have agreements? How did formal agreements with defined roles and responsibilities impact response operations?
   b. If no, has there been discussion within your organization to establish formal agreements? What factors prevent forming formal agreements?
5. How does your department/agency maintain and share information on the current status of its primary, secondary, and backup communications capabilities?
6. Has your department/agency implemented or explored sharing communications systems and infrastructure or Shared Communications Systems and Infrastructure?
   a. If so, does your department/agency have any ongoing sharing agreements in

place with other emergency communications partners? What are the agreements for (e.g., sharing network system, sharing infrastructure, joint talk-groups, etc.)?

b. Does your department/agency actively participate in the ECPC's Federal Resource Sharing Working Group?

Technology and Infrastructure

1. In 2022, what type of new technology solutions has your department/agency implemented to enhance interoperability or continuity of communications?
2. How does your department/agency evaluate new communications technologies (e.g., annual review, market research, testing) to ensure interoperability with existing systems?
    a. Has your department/agency engaged in any emergency communications related research and development activities?
3. In 2022, how many times did your department/agency use commercial off-the-shelf (COTS) solutions to close a capability gap? Can you provide the names of the COTS used and for what purpose?
    a. If yes, what factors influenced your department/agency's decision to rely on a COTS solution?
4. In 2022, did your organization conduct any pilot or other communications research and development projects with federal partners?
5. Has your department/agency incorporated 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?
6. Has your department/agency deployed unmanned aerial systems (UAS) to support emergency communications or response operations?

Cybersecurity

1. In 2022, how did your department/agency share cybersecurity threat information (e.g., e-mail updates, partner meetings, Information Technology department, etc.) with other federal, state, local, tribal, and territorial (FSLTT) partners? What benefits did sharing cybersecurity information provide to your department?
    a. Are there barriers hindering better cybersecurity information sharing (e.g., classification, networking requirements, etc.)? If there are barriers, what action would help eliminate them?
2. Does your department/agency's current communications strategic/operational planning process include cybersecurity incident response and vulnerability response plans?
    a. If no, how would your organization respond to a cybersecurity incident that impacted emergency communications systems?

3. In 2022, did your department/agency's cybersecurity assessments identify any emergency communications equipment or system specific cybersecurity vulnerabilities?
    a. If yes, how did your department/agency address communications equipment or system vulnerabilities?
    b. If no, how does your department/agency assess existing/future communications systems for cybersecurity vulnerabilities?
4. In 2022, how many disruptions to communications during response operations (e.g., radio-frequency jamming or interference) did your department/agency experience? What steps did your department/agency take to identify and mitigate those vulnerabilities?
5. Federal departments and agencies are required to implement the National Institute of Standards and Technology (NIST) cybersecurity standards to protect their networks. How has the implementation of the NIST cybersecurity standards, or similar standards, impacted communications interoperability?

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 2022 ASA a tracking mechanism, Section III Summary of 2022 ASA Findings and Recommendations.