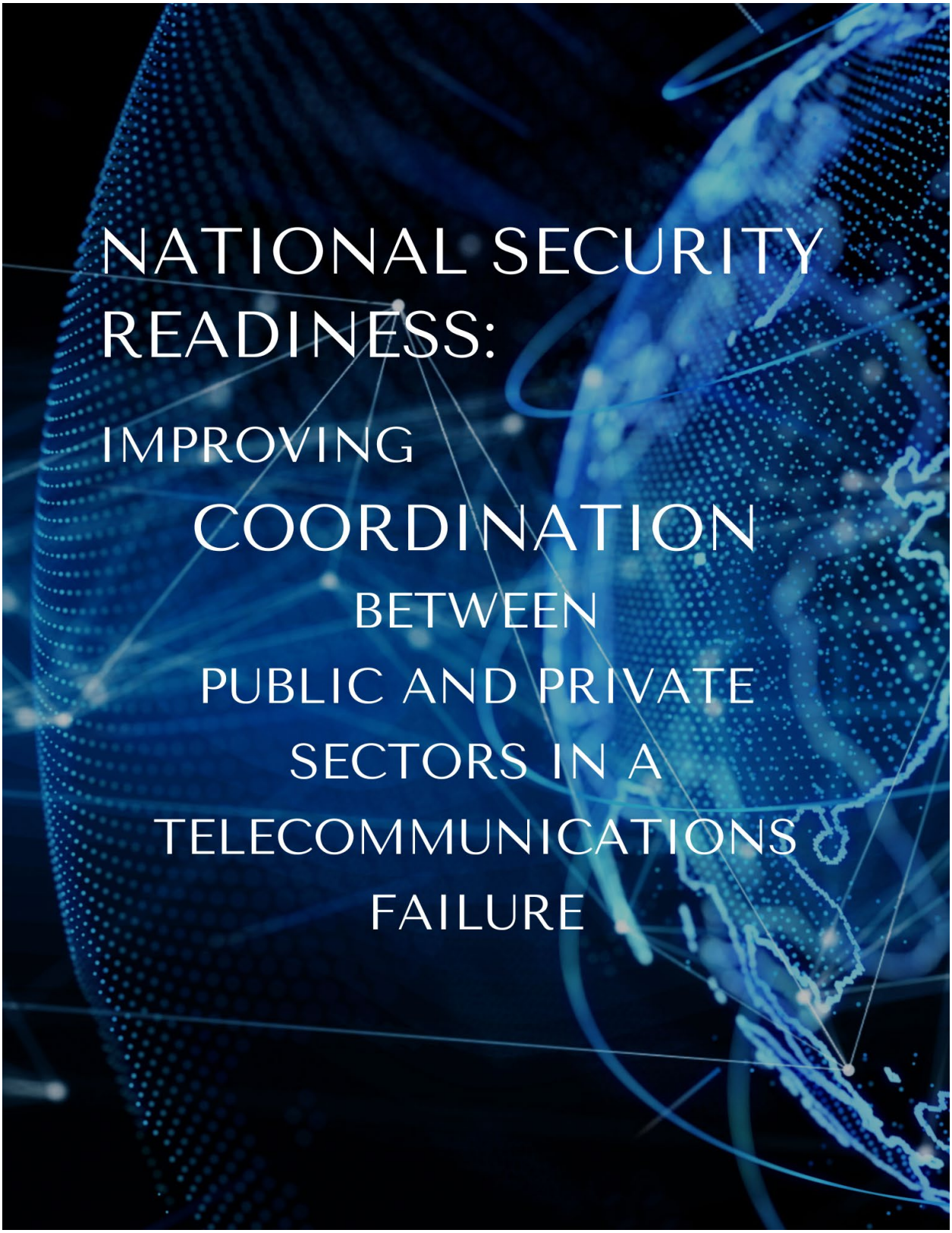


NATIONAL SECURITY READINESS:

IMPROVING COORDINATION BETWEEN PUBLIC AND PRIVATE SECTORS IN A TELECOMMUNICATIONS FAILURE

2023 PUBLIC-PRIVATE ANALYTIC EXCHANGE PROGRAM

National Security Readiness Team

Participants

Name	Affiliation
Jessica C.	Crisis24
Briana F.	Guidehouse
Seamus L.	Meridian Strategic Services
Jennifer L.	Federal Emergency Management Agency
Francisco R.	Department of the Treasury
Amanda S.	Office of the Director of National Intelligence
Allyson S.	Peraton
Morgan W.	Coast Guard
Feroza Y.	Department of the Treasury

Champions

Name	Affiliation
Sharon Halstead	ODNI, then Equal Employment Opportunity Commission
Johnny Starrunner	Federal Bureau of Investigation

Homeland Security

National Security Readiness: Improving Coordination Between Public and Private Sectors in a Telecommunications Failure

Overview

In today's increasingly complex threat landscape, our national security readiness will be better postured through increased public and private sector communication and coordination, especially with critical infrastructure incidents. Our group convened to address national security resilience and readiness as part of the Analysts Exchange Program (AEP).

A review of over seventy after-action reports from exercises and real-world incidents nationwide impacting critical infrastructure between 2008 and 2022 demonstrated the loss of communications as a critical issue. It highlighted the need for redundant interoperable communications capabilities. In addition, our team conducted a series of interviews and completed surveys with both public and private sector individuals, showing a consensus that while communication and coordination are only sometimes strong, it is nevertheless a desired path for future development and security planning. The group conducted a literature review, analysis of after-action reports, interviews with stakeholders, and a nationwide cross-industry survey as methods to inform recommendations.

The group determined a significant need for more public-private sector collaboration and four potential opportunities to enhance communication and coordination: collaborative capacity building, data sharing and analysis, increased engagement with professional associations and industry groups, and determining shared objectives and outcome measurement.

Key Findings

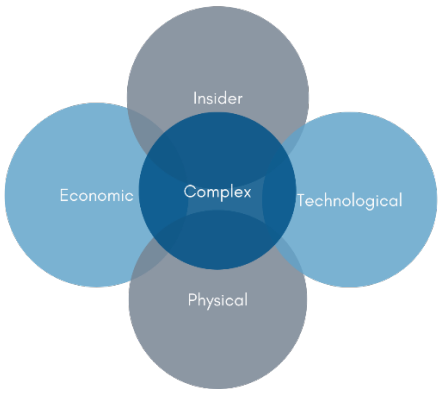
Improving public-private sector communication and coordination is vital to national security readiness, particularly in critical infrastructure sectors. We focused on the high-impact, low-probability scenario of traditional communication channels failing, a risk commonly shared by all sectors and industries. We identified a cross-industry baseline of communication plans and evaluated barriers to public-private sector communication and coordination and organizational ability to adapt to threats. A literature review, analysis of after-action reports, interviews with stakeholders, and a nationwide cross-sector survey informed our findings.

Communication Plans Require Assessment and Redundancies

In our thematic after-action review, the main themes in the areas for improvement stemmed from the loss of communications capabilities and stakeholder communications, such as the need for alternate communication methods and differing organizational priorities. The strengths were prioritization bolstered by multiple communication channels, which enabled the identification of at-risk critical infrastructure and alternate forms of communication.

Based on stakeholder input, we characterized the threat landscape into five categories: economic, internal, physical, technological, and complex threats. Although we cannot evaluate true readiness to threats, our respondents perceived that their organizations were prepared and agile in a changing threat environment.

Interconnection of Complex Threats Within the Five Categories



When communications failed, our respondents reported having a plan that had been evaluated with redundancy built into their communications systems.

Less than half of our respondents had a nationwide communications capability, and less than a third had collaborated across their industry to assess interoperability.

Redundancies Were Overly Dependent on Traditional Channels

In our baseline readiness survey, our stakeholder interviewees and survey respondents shared what technology they plan to use to communicate when traditional channels fail. About half of the responses were either still defined as traditional channels or needed to be timelier. The federal government and the private sector offer alternate methods of communication if landline or cellular networks are unavailable. These methods include dedicated networks, mass notification systems, radios, and satellite phones.[4][5][6][7]

Fifty-one percent of respondents said their organizations' engagement with their public or private sector counterparts was either none, minimal, or only as required by law.

Given this lack of public-private sector cross-pollination, four opportunities to enhance communication and coordination include capacity building, data sharing and analysis, greater engagement with professional associations and industry groups, and shared objectives and outcome measurement.[8][9][10][11][12][13][14][15][16][17][18][19]

The critical barriers to coordination and connecting with public and private partners stem from a need for existing relationships between the two sectors. The main barriers to adapting to an evolving threat environment stem from knowledge gaps, resource constraints, and differing prioritizations.[20][21][22][23][24][25][26][27][28][29][30][31]

Methodology

We used a four-pronged approach to identify, research, and evaluate a pervasive, nationwide problem within national security readiness.

Literature Review

We reviewed nearly 40 sources, including documentaries, documentation for alternate communication methods, emergency management training, federal government resources, journal articles, press reporting, state government public safety plans, and more to inform our research plan. These sources covered topics such as identifying at-risk infrastructure during an incident response, designing a communications plan, federal agencies involved in emergency communications, available technology during a disaster, emergency services technology platforms, and alternate methods of communication.

Thematic After-Action Review

We examined over seventy after-action reports from exercises and real-world incidents nationwide impacting critical infrastructure between 2008 and 2022 for common strengths and areas for improvement.

Stakeholder Interviews

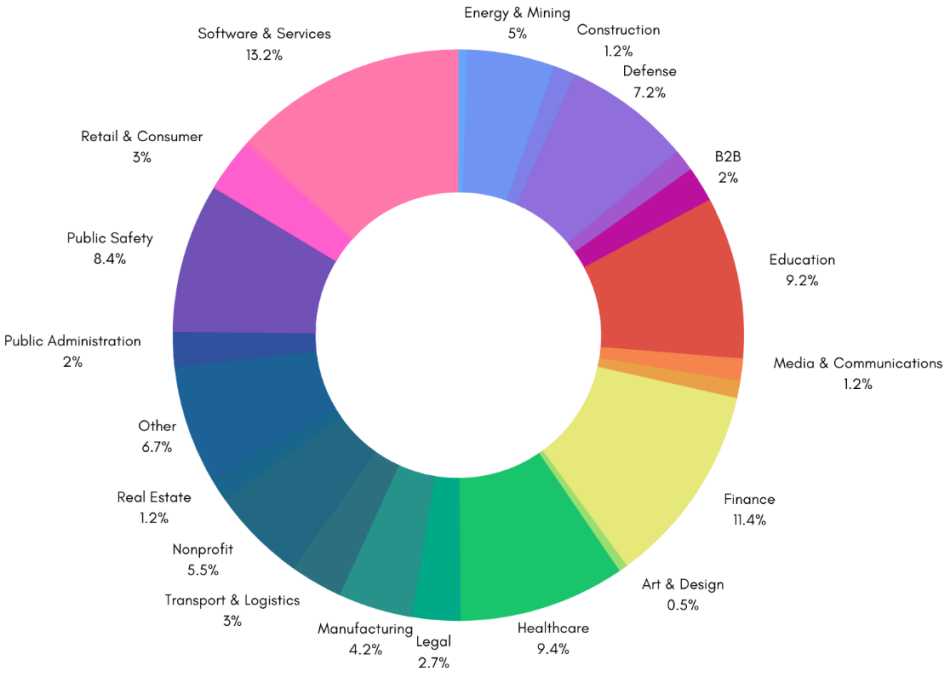
We interviewed eleven stakeholders for anonymous, detailed input on baselining communication plans, nationwide and industry interoperability, private and public sector communication, and evaluating threats for multiple industries. These stakeholders represented several sectors: academia, cyber and information technology, emergency management, pharmaceutical/chemical, transportation/logistics, and utilities. , , , , , , , , , ,

Nationwide Survey

We received over four hundred responses from an anonymous survey to gather cross-sector input on baselining communication plans, nationwide and industry interoperability, private and public sector communication, and evaluating threats. The survey included demographic questions, closed-ended questions, open-ended questions, and Likert scales, all designed using social science survey methodology.

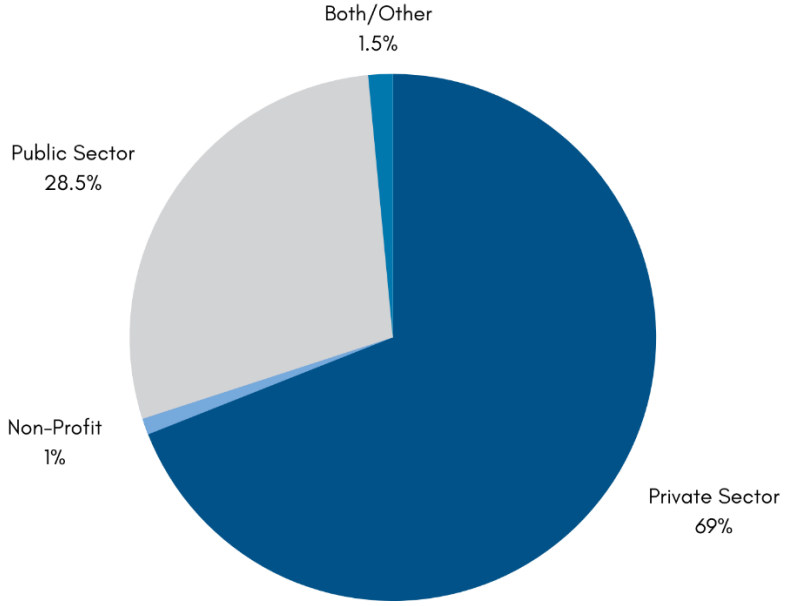
Twenty-six industries are represented in the data, with the top five selected including software and information technology services, financial services, healthcare, education, and public safety.

Survey Responses Representing Diverse Sectors and Industries



Approximately 29% of respondents were from public sector organizations, 69% from private sector organizations, and 2% included non-profits and public-private partnerships.

Survey Response Represented a Diverse Group of Organizations



Thematic After-Action Review Informs Research Direction

In our thematic after-action review, our analysis deliberately covered a range of threats -- including active shooters, cyber-attacks, mass power outages, and natural disasters-- across all levels of government to provide a cross-cutting perspective on pervasive areas for improvement and strengths applicable to the broadest audience.

The main themes found in the areas for improvement stemmed from the loss of communications capabilities and stakeholder communications. Examples of areas for improvement are below.

- *Alternate communication methods*, especially with potential cascading events within one incident.
- *Centralized information sharing location* for situation awareness with information such as personnel resources and equipment.
- *Differing organizational priorities* between the public and private sectors – for example, the public sector protects life and property while the private sector restores power.
- *Lack of interoperable or backup communication systems* hindered a unified incident response.

The main themes found in the strengths were prioritization bolstered by multiple channels of communication and public-private sector cooperation. Examples of strengths are below.

- *Identification of at-risk critical infrastructure,* with the assistance of CISA, during incident response to help prioritize emergency repairs.
- *Invest in alternate methods of communication,* such as portable radios and satellite phones.

- *Prioritization of emergency repairs to overcome the loss of communications,* including information from multiple channels such as field assessments, satellite phones, community engagement, and crowdsourcing.
- *Use of the United States Air Force Military Auxiliary Radio System (MARS),* contingency communications support for national security missions.

Characterizing The Threat Landscape

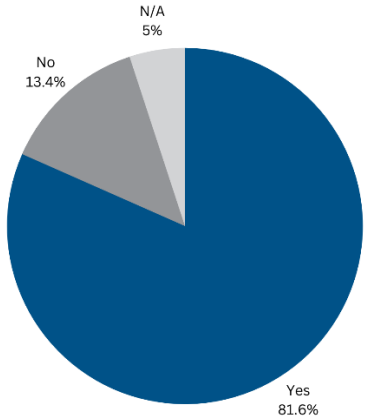
To test our hypothesis about threats to our national security readiness and interconnectedness to telecommunications, we asked our stakeholder interviewees and survey respondents to share the top threats to their organization. We categorized the responses into five types: economic threats impacting financial or business operations, internal threats affecting organization growth, physical threats influencing workforce safety or property loss, technological threats predominantly from cyber actors or digital networks, and cross-cutting threats that could fall into two or more of the other categories. The five categories with example threats are provided below.

1. *Economic Threats:* cost of materials from state actors, delays in supply chain logistics, identity theft, intellectual property theft, and industrial espionage, volatility in financial systems,
2. *Internal Threats:* insider threats, aging of the workforce, talent recruitment,
3. *Physical Threats:* active shooters, workplace violence,
4. *Technological Threats:* artificial intelligence developments such as deep faking a client's voice, cloud outage, communications failure, data breach and loss, distributed denial-of-service, hackers, phishing, ransomware, social engineering, zero-day exploits, ,
5. *Cross-cutting Threats:* civil unrest, climate change, insider threat, natural disasters, power failures, state actors, terrorism, ,

Weighted List of Threats Identified

Approximately 80% of our survey respondents indicated they had a plan to address the threats facing their organization, with 85% perceiving their organization was adapting on average or higher than average to the evolving threat environment. Although we cannot evaluate actual readiness to threats, our respondents perceived that their organizations were prepared and agile in a changing threat landscape.

Responses About Having a Plan



Baseline Readiness in The Event of a Communications Failure

We defined a communications failure as an incident where an organization cannot access traditional communication channels such as email, cell phone, or third-party platforms such as Slack, Adobe Connect, or Zoom. Depending on the cause, this communication failure could last from minutes to days to weeks. We asked our stakeholder interviewees and

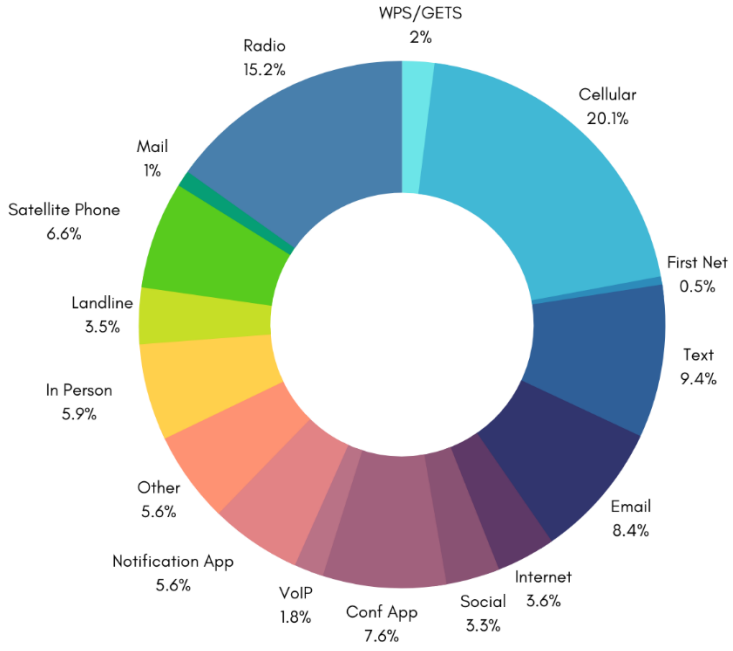
survey respondents a series of questions to baseline their communications plans and nationwide and industry interoperability in case of a communications failure.

Sixty-nine percent of respondents had a plan during a communications failure.
Seventy-five percent of respondents had tested this plan.
Sixty-five percent of respondents had redundancy built into their communications systems.
Thirty-nine percent of respondents had a nationwide communications capability.
Thirty percent of respondents had collaborated across their industry to test interoperability.

Resources For More Robust Alternate Methods of Communication

In our baseline readiness survey, our stakeholder interviewees and survey respondents shared what technology they plan to use to communicate when traditional channels fail. About half of the responses were defined as conventional channels —such as cellular, text, email, and third-party platforms— or were admittedly untimely such as mail or in-person via runners when not co-located.

Planned or Noted Redundancies in a Telecommunications Failure



The federal government and the private sector offer several alternate methods of communication if landline or cellular networks are unavailable. These methods include dedicated networks, mass notification systems, radios, and satellite phones. Many redundant methods rely on terrestrial fiber, cellular, or satellite capabilities—few referenced mesh connectivity using Bluetooth or other short-range communication methods.

Federal Government Programs

The Cybersecurity and Infrastructure Security Agency (CISA) administers three priority telecommunications services to aid essential personnel in national security and emergency response activities, with similar alternative network options available by private sector companies.

- *Government Emergency Telecommunications Service (GETS)* prioritizes calls on landline networks. GETS is a White House-directed emergency telephone service provided and managed by CISA. GETS gives subscribers priority access and processing in landline telephone networks' local and long-distance segments. Subscribers are issued a Personal Identification Number (PIN) that assigns priority status to calls in service provider networks when used. Calls made with GETS overcome network congestion and degradation and complete connections with a success rate of 98%. GETS calls do not preempt calls in progress or deny the general public's telephone network use.
- *Wireless Priority Service (WPS)* is a program that authorizes cellular communications service providers to prioritize calls over wireless networks when congested. .
- *Telecommunications Service Priority (TPS)* is a Federal Communications Commission (FCC) program that directs telecommunications service providers (e.g., wireline and wireless phone companies) to give preferential treatment to users enrolled in the program when they need to add new lines or have their lines restored following a disruption of service, regardless of the cause. Enrollment in TPS ensures that wireline circuits are restored on a priority basis.

CISA advances public safety interoperable communication capabilities through its *Interoperable Communications Technical Assistance Program.* This program directly supports state, local, tribal, and territorial government entities through training, tools, and onsite assistance.

Mass notification systems broadcast real-time alerts to a substantial number of individuals. A unique public-private partnership between the Federal Emergency Management Agency (FEMA), the FCC, and the wireless industry operationalizes the *Wireless Emergency Alerts* (WEA) system for national, state, or local government authorities to use in public safety emergencies. Over a dozen mass notification system options are available from private sector companies.

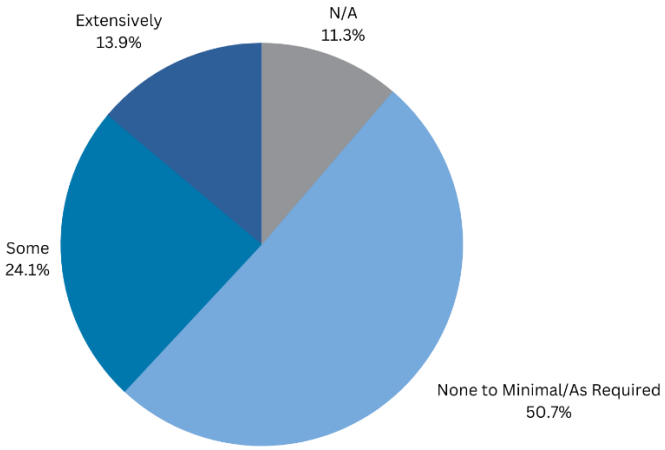
The *Military Auxiliary Radio System (MARS)* is a Department of Defense-sponsored program for volunteer licensed amateur radio operators to provide emergency communications to local, national, and international public safety organizations. The radio operators possess a valid FCC amateur radio license and the capability to transmit on MARS high frequencies.

The *SHAred RESources (SHARES) High-Frequency Radio* program, open to national security and emergency management users performing critical functions, uses existing high-frequency radio resources to communicate when landline and cellular communications are unavailable.

Opportunities For Enhancing Communications and Coordination

Fourteen percent of respondents reported that their organizations' level of coordination and communication with federal, state, local, tribal, and territorial (FSLTT) government was extensive. Moreover, fifty-one percent of respondents said their organizations' engagement with their public or private sector counterparts was either none, minimal, or only as required by law.

Coordination with FSLTT Partners on Communications



Given this lack of public-private sector collaboration, four potential opportunities to enhance communication and coordination include capacity building, data sharing and analysis, greater engagement with professional associations and industry groups, and shared objectives and outcome measurement.

Provide Capacity Building Workshops

Offer capacity-building workshops to enhance public and private sector professionals' understanding, skills, and capabilities. The public sector could provide industry-specific contact sheets with short explanations for how each role collaborates with the private sector. For each role, the public sector could use a position email rather than a specific point of contact's email to improve consistency in employee turnover.

Increased Data Sharing and Analysis with Trusted Partners

Encourage sharing of relevant data between the private and public sectors while respecting privacy and security concerns. Analyze data collectively to identify trends, gaps, and opportunities, enabling evidence-based decision-making and policy formulation.

Engage Professional Associations and Industry Groups as Intermediaries

Collaborate with professional associations and industry groups that represent the private sector. Industry-specific committees should reflect the perspectives of large, mid-size, and small businesses. These organizations can serve as intermediaries, facilitating communication, coordination, and knowledge sharing between the private and public sectors on issues related to policy, regulation, industry trends, and emerging challenges.

When appropriate, encourage joint public-private initiatives, projects, and investments that leverage the strengths of both sectors.[,,,]

Share Objectives and Outcome Measurement

Align the objectives and outcomes of the private and public sectors to facilitate effective collaboration. Define shared goals and measurement frameworks that encourage mutual accountability and evaluation of collaborative initiatives. Encourage both parties to think beyond typical considerations or limit solutions to geographical boundaries or outdated checklists.[,]

Barriers To Effective Public-Private Communication and Coordination

Critical barriers to coordinating and connecting with public and private partners stem from a need for existing relationships between the two sectors. Examples of noted challenges are listed below.

- *Allotting Time* to maintain these relationships with a minimal workforce on top of regular day-to-day duties.[,,]
- *Determining Proper Points of Contact* for the necessary counterparts without it being previously established or maintained.[,,,,,]
- *Fear of Sharing Information* due to differences in data classification, access controls, clearances, and non-disclosure agreements.[,]
- *Guaranteeing Participation* between the two sectors remains challenging with a lack of knowledge in initiating communications, definition of roles, and available capabilities.[,,]
- *Limited Buy-In* from executives leads to insufficient funding to fulfill up-to-date approaches to the threat picture.

Differing Prioritization and Other Barriers to Effective Threat Management

The main barriers to adapting to the threat environment stem from differing prioritizations, knowledge gaps, and resource constraints. Examples of noted challenges are listed below.

- *Lack of Understanding* of the cyber threat landscape and its threat probability on entities.
- *Minimal Resources* are allotted to both sectors to prepare against the threat environment. These resources include, but are not limited to, information access, executive support, maintaining trend analysis and awareness, proper financing, qualified personnel, and technology.[,,,,,]
- *Misaligned Priorities* with a centralized focus on short-term success rather than preparing for long-term resiliency.[,]
- *Unclear or Lack of Transparency in Vetting Policies* for hiring employees in the critical infrastructure sectors who are citizens of a country hostile to the United States due to increased insider threat risk.

Potential Research for Future AEP Programs

While this project provided initial research and a glimpse into national security vulnerability related to telecommunications failures, future AEP groups could develop frameworks or

materials for preparing a mitigation or recovery plan for a telecommunications failure that included redundancies. An assessment or presentation of alternative communications methods upon loss or degradation of traditional terrestrial fiber, cellular, or satellite channels.

Analytic Deliverable Dissemination Plan

Office of the Director of National Intelligence
FBI, including the Domestic Security Alliance Council and Infragard
Intelligence Community Outreach Coordinators
Federal Communications Commission
Department of Homeland Security and Component Organizations
BENS
FBI Intelligence Analysts Association
Department of the Treasury
Equal Employment Opportunity Commission
Financial Oversight Bodies
Federal Emergency Management Agency
Crisis 24
Guidehouse
Meridian Strategic Services
Peraton
Individual Interview Subjects and Participating Organizations

Disclaimer Statement

This document is provided for educational and informational purposes only. The views and opinions expressed in this document do not necessarily state or reflect those of the United States Government or the Public-Private Analytic Exchange Program, and they may not be used for advertising or product endorsement purposes. All judgments and assessments are solely based on unclassified sources and the product of joint public and private sector efforts.