United States Government Accountability Office

Report to Congressional Addressees

November 2021

CRITICAL INFRASTRUCTURE PROTECTION

CISA Should Assess the Effectiveness of its Actions to Support the Communications Sector

GAO@100
A Century of Non-Partisan Fact-Based Work

GAO-22-104462

GAO@100 Highlights

Highlights of GAO-22-104462, a report to congressional addressees

November 2021

CRITICAL INFRASTRUCTURE PROTECTION

CISA Should Assess the Effectiveness of Its Actions to Support the Communications Sector

Why GAO Did This Study

The Communications Sector, one of 16 critical infrastructure sectors, is vital to the United States. Its incapacitation or destruction could have a debilitating impact on the safety and security of our nation. The private sector owns and operates the majority of communications infrastructure, including broadcast, cable, satellite, wireless, and wireline systems and networks. DHS's CISA is the lead federal agency responsible for supporting the security and resilience of the sector.

GAO examined (1) the security threats CISA has identified to the sector, (2) how CISA supports the sector, and (3) the extent to which CISA has assessed its support and emergency preparedness for the sector. GAO reviewed DHS reports, plans, and risk assessments on the sector and interviewed CISA officials and private sector stakeholders to identify and evaluate CISA's actions to support the security and resilience of the Communications Sector.

What GAO Recommends

GAO is making three recommendations to CISA, including that CISA assess the effectiveness of its support to the Communications Sector, and revise its *Communications Sector-Specific Plan*. The Department of Homeland Security concurred with the recommendations. The Department of Commerce and the Federal Communications Commission did not provide comments on the draft report.

View GAO-22-104462. For more information, contact Leslie V. Gordon at (202) 512-8777 or GordonLV@gao.gov.

What GAO Found

The Communications Sector is an integral component of the U.S. economy and faces serious physical, cyber-related, and human threats that could affect the operations of local, regional, and national level networks, according to the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and sector stakeholders.

Examples of Potential Security Threats to the Communications Sector

Type of threat	Description
Physical	• Natural occurrences, such as hurricanes, floods, and ice storms • Human-made occurrences, such as explosive, chemical, biological, or radiological contaminant attacks on communications network infrastructure and personnel
Cyber-related	• Malicious actors, such as adversaries who intentionally disrupt the systems on a communications network • Nonmalicious actors, such as employees that accidentally alter a communication network's configuration, negatively affecting the network's ability to function properly
Human	• Threats to a communications network due to the failure of employees to plan for security incidents and implement protocols to protect networks from the impacts of such incidents

Source: GAO analysis of Department of Homeland Security documentation. | GAO-22-104462

In addition, CISA determined that the Communications Sector depends on other critical infrastructure sectors—in particular, the Energy, Information Technology, and Transportation Systems Sectors—and that damage, disruption, or destruction to any one of these sectors could severely impact the operations of the Communications Sector.

CISA primarily supports the Communications Sector through incident management and information-sharing activities, such as coordinating federal activities to support the sector during severe weather events and managing cybersecurity programs, but has not assessed the effectiveness of these actions. For example, CISA has not determined which types of infrastructure owners and operators (e.g., large or small telecommunications service providers) may benefit most from CISA's cybersecurity programs and services or may be underrepresented participants in its information-sharing activities and services. By assessing the effectiveness of its programs and services, CISA would be better positioned to identify its highest priorities.

CISA has also not updated the 2015 *Communications Sector-Specific Plan*, even though DHS guidance recommends that such plans be updated every 4 years. As a result, the current 2015 plan lacks information on new and emerging threats to the Communications Sector, such as security threats to the communications technology supply chain, and disruptions to position, navigation, and timing services. Developing and issuing an updated plan would enable CISA to set goals, objectives, and priorities that address threats and risks to the sector, and help meet its sector risk management agency responsibilities.

Contents

Letter		1
	Background	5
	CISA Has Identified Physical, Cyber-related, and Human Threats to the Communications Sector	12
	CISA Supports the Security and Resilience of the Communications Sector through Incident Management and Information-Sharing	19
	CISA Has Not Assessed Its Support to the Communications Sector nor Updated Its Sector Plan	24
	Conclusions	30
	Recommendations for Executive Action	31
	Agency Comments	31
Appendix I	Comments from the Department of Homeland Security	34
Appendix II	GAO Contact and Staff Acknowledgments	38

Tables

	Table 1: Five Industry Segments of the Communications Sector	6
	Table 2: Physical Threats and Potential Impacts to the Communications Sector Identified by the Department of Homeland Security (DHS)	13
	Table 3: Cyber-related Threats and Potential Impacts to the Communications Sector Identified by the Department of Homeland Security (DHS)	15
	Table 4: Human Threats and Potential Impacts to the Communications Sector Identified by the Department of Homeland Security (DHS)	17
	Table 5: Communications Sector Critical Dependencies Identified by the Department of Homeland Security (DHS)	18
	Table 6: Department of Homeland Security (DHS) Communications Sector Strategic Initiatives	23

Figure

	Figure 1: Key Components of the Communications Sector's Systems and Technology	8

Abbreviations

5G	fifth generation
CISA	Cybersecurity and Infrastructure Security Agency
DHS	Department of Homeland Security
EMP	electromagnetic pulse
FEMA	Federal Emergency Management Agency
Framework	National Response Framework
GMD	geomagnetic disturbance
GPS	Global Positioning System
ICT	information and communications technology
National Plan	National Infrastructure Protection Plan
PNT	positioning, navigation, and timing
SCRM	supply chain risk management

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

441 G St. N.W.
Washington, DC 20548

November 23, 2021

The Honorable Bennie G. Thompson
Chairman
The Honorable John Katko
Ranking Member
Committee on Homeland Security
House of Representatives

The Honorable Frank Pallone, Jr.
Chairman
The Honorable Cathy McMorris Rodgers
Republican Leader
Committee on Energy and Commerce
House of Representatives

The Communications Sector—comprised of broadcast, cable, satellite, wireless, and wireline systems and networks primarily owned and operated by the private sector—is an integral component of the U.S. economy and vital to national security. It underlies the operations of businesses, public safety organizations, and government. The federal government has identified the sector as part of critical infrastructure protection efforts because its incapacitation or destruction could have a debilitating impact on the safety and security of our nation.[1] For example, in 2017, Hurricane Maria severely damaged communications critical infrastructure in Puerto Rico and in the U.S. Virgin Islands, leaving residents without reliable and continuous access to voice and data communications. Without telecommunication services, people were unable to call for help during medical emergencies and receive mobile weather alerts on floods and landslides. The federal government works with private sector owners and operators to predict, anticipate, and respond to sector outages and assist response and recovery efforts to enable communications during times of crisis.

The Cybersecurity and Infrastructure Security Agency Act of 2018 established the Cybersecurity and Infrastructure Agency (CISA) as an

[1]Presidential Policy Directive 21 established national policy on critical infrastructure security and resilience for the nation's 16 critical infrastructure sectors. See White House, *Presidential Policy Directive 21: Critical Infrastructure Security and Resilience* (February 2013).

operational component agency within the Department of Homeland Security (DHS).[2] The act assigned CISA the responsibility to enhance the security of the nation's critical infrastructure in the face of both physical and cyber threats, among other responsibilities. CISA is the lead federal agency, or sector risk management agency, for the Communications Sector and is responsible for coordinating efforts to protect and improve the sector's security and resilience.[3] The National Defense Authorization Act for Fiscal Year 2021 identifies a number of responsibilities for sector risk management agencies, including CISA. These responsibilities include supporting critical infrastructure owners and operators by identifying threats, assessing sector risks, sharing information, and supporting incident management and restoration efforts during or following an incident, such as a hurricane.[4]

In our prior work, we have highlighted a variety of challenges CISA has faced in managing its roles and responsibilities to support the security and resilience of the nation's critical infrastructure.[5] Most recently, in March 2021, we reported that government and private sector critical infrastructure stakeholders supported by CISA's three primary mission areas—protecting networks, critical infrastructure protection, and emergency communications—identified challenges in coordinating with

[2]Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. No. 115-278, §2, 132 Stat. 4168, 4169 (codified at 6 U.S.C. § 652).

[3]In January 2021, the National Defense Authorization Act for Fiscal Year 2021 established "sector risk management agency" responsibilities for federal departments or agencies designated as such for each critical infrastructure sector or subsector. See Pub. L. No. 116-283, § 9002(c). Prior to enactment of the act, a "sector risk management agency" was called a "sector-specific agency." See Pub. L. No. 116-283, § 9002(a)(7).

[4]See Pub. L. No. 116-283, § 9002(c). An incident is an occurrence, natural or human-made, that necessitates a response to protect life or property and includes planned events as well as emergencies or disasters of all kinds and sizes. See Federal Emergency Management Agency, *National Incident Management System*, 3rd ed. (October 2017); and Department of Homeland Security, *National Response Framework,* 4th ed. (Oct. 28, 2019).

[5]For example, see GAO, *Critical Infrastructure Protection: Actions Needed to Enhance DHS Oversight of Cybersecurity at High-Risk Chemical Facilities*, GAO-20-453 (Washington, D.C.: May 14, 2020).

CISA.[6] For example, some of these stakeholders said CISA had inconsistently distributed information, and it had not provided timely responses to stakeholder requests. As a result, we made a number of recommendations, including that CISA take steps to ensure that organizational changes are aligned with the needs of stakeholders, that these stakeholders know with whom they should be coordinating in CISA's organization, and that appropriate parties are included in distribution lists or other communications channels.[7]

We performed our current work under the authority of the Comptroller General to conduct evaluations of government activities.[8] Our work reviewed CISA's efforts to support the security and resilience of the Communications Sector. Specifically, this report examines (1) the security threats CISA has identified, (2) CISA's support of the sector, and (3) the extent to which CISA has assessed its support and emergency preparedness for the sector.

To address all three objectives, we reviewed federal policies, DHS documentation, and our prior work on critical infrastructure protection to select a subset of federal agencies and a nongeneralizable sample of private sector entities representing the five industry segments of the Communications Sector—broadcast, cable, satellite, wireless, and wireline.[9] Specifically, we selected and interviewed officials from the following federal agencies with roles and responsibilities in the sector: DHS, the Department of Commerce, and the Federal Communications Commission. We also selected and interviewed representatives from 11

[6]GAO, *Cybersecurity and Infrastructure Security Agency: Actions Needed to Ensure Organizational Changes Result in More Effective Cybersecurity for Our Nation*, GAO-21-236 (Washington, D.C.: Mar. 10, 2021). Selected stakeholders included 16 critical infrastructure stakeholders (eight representatives of selected Sector Coordinating Councils and eight representatives from selected Government Coordinating Councils), six federal Chief Information Officers, and six Statewide Interoperability Coordinators and other emergency communications stakeholders.

[7]DHS concurred with our recommendations and, as of September 2021, CISA was in the process of taking action to address them. We will continue to monitor CISA's progress to address the recommendations.

[8]31 U.S.C. § 717(b).

[9]Specifically, we reviewed federal roles and responsibilities for critical infrastructure security and resilience in Presidential Policy Directive 21. See White House, *Presidential Policy Directive 21*. We also used our prior work on critical infrastructure protection to identify agencies and organizations that are members of councils relevant to the Communications Sector.

private sector entities.[10] The information gathered provided examples of perspectives on threats to the Communications Sector and on CISA's actions to support sector security and resilience; however, the information obtained from these interviews is not generalizable to all federal agencies or Communications Sector private sector entities.

To address our first objective, we reviewed DHS reports, plans, and risk assessments on the Communications Sector. In particular, we reviewed DHS's *2012 Risk Assessment Report for Communications* and the 2015 *Communications Sector-Specific Plan*, which CISA officials told us describe continuing and relevant threats to the Communications Sector.[11] We also met with CISA officials with roles and responsibilities for supporting Communications Sector security and resilience, including those from the National Risk Management Center and the Stakeholder Engagement Division, to obtain their perspectives on current and relevant threats to the sector.

To address our second and third objectives, we collected and analyzed DHS and CISA reports, strategies, plans, guides, briefings, and assessments on CISA's related activities in support of communications critical infrastructure security and resilience. We also interviewed officials from CISA's Cybersecurity Division, Emergency Communications Division, Infrastructure Security Division, Integrated Operations Division, National Risk Management Center, and Stakeholder Engagement Division to discuss services and products offered to the Communications Sector to support security and resilience efforts. We compared the actions CISA took to assess its support for the Communications Sector against guidance from the *National Infrastructure Protection Plan*, the *Communications Sector-Specific Plan*, and the *DHS Critical Infrastructure*

[10]We interviewed representatives from the following private sector entities: ACA Connects, AT&T, CTIA-the Wireless Association, Communications Information Sharing and Analysis Center, Communications Sector Coordinating Council, National Association of Broadcasters, NCTA-the Internet & Television Association, NTCA-the Rural Broadband Association, Pioneer, Satellite Industry Association, and Telecommunications Industry Association.

[11]Department of Homeland Security, *2012 Risk Assessment Report for Communications* (Sept. 27, 2012); and *Communications Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan 2013* (2015). Both of these reports were the most recent DHS reports available on the Communications Sector during the time of our review.

Risk Management Framework.[12] We also assessed CISA's preparedness activities to coordinate Communications Sector incident management and restoration efforts against Federal Emergency Management Agency (FEMA) guidance on Emergency Support Function preparedness—key response coordinating structures at the federal level for incidents such as hurricanes and wildfires.[13]

We conducted this performance audit from September 2020 to November 2021 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Overview of the Communications Sector

Communications is one of seven "community lifeline" services that enables the continuous operation of critical government and business functions and is essential to human health and safety and economic security.[14] The Communications Sector includes five industry segments—broadcast, cable, satellite, wireless, and wireline. For an overview of each of the five industry segments of the Communications Sector, see table 1 below.

[12]Department of Homeland Security, *Communications Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan 2013*; *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (December 2013); and *Supplemental Tool: Executing A Critical Infrastructure Risk Management Approach* (2013).

[13]As discussed later in this report, CISA is designated as the federal coordinator for Emergency Support Function #2, which supports government and industry efforts to restore critical communications infrastructure and services during incidents (e.g., hurricanes and wildfires), facilitate the stabilization of systems and applications from malicious activity (e.g., cyber), and coordinate communications support to response efforts such as emergency alerts and telecommunications. Within DHS, FEMA is responsible for guiding and supporting other departments and agencies, like CISA, in conducting their national preparedness activities. See Department of Homeland Security, Federal Emergency Management Agency, *Memorandum for Emergency Support Function Leadership Group - Performance Metrics for Emergency Support Function Preparedness* (June 30, 2015).

[14]Community lifeline services are the most fundamental services in the community that, when stabilized, enable all other aspects of society to function. There are seven Community lifeline services: safety and security; food, water, and shelter; health and medical; energy; communications; transportation; and hazardous material.

Table 1: Five Industry Segments of the Communications Sector

Industry segment	Description
Broadcast	Consists of free and subscription-based, over-the-air radio and television stations that offer audio and video programming services and data services
Cable	Consists of systems that offer video programming services, digital telephone service, and high-speed broadband services
Satellite	Includes platforms launched into orbit to serve a variety of functions, such as the bidirectional transmission of voice, video, and data services; data collection; event detection; timing; and navigation
Wireless	Refers to telecommunication services in which spectrum is used to carry signals over part of, or the entire, communications path[a]
Wireline	Refers to wired connections that include private enterprise data and telephone networks, the core backbone of the internet and public switched telephone networks

Source: Department of Homeland Security information. | GAO-22-104462

[a]Spectrum is the range of all frequencies of electromagnetic radiation that are subdivided into frequency bands used by a wide variety of technologies, including communications technology, to operate. In addition to the wireless industry segment, the broadcast and satellite segments also use spectrum.

The systems and technology underlying the Communications Sector consist of numerous interconnected networks that provide the basis for the operation of the internet and telecommunications services. Communications networks involve both physical infrastructure (buildings, switches, towers, antennas, etc.) and cyber infrastructure (software, operational support systems, user applications, etc.).

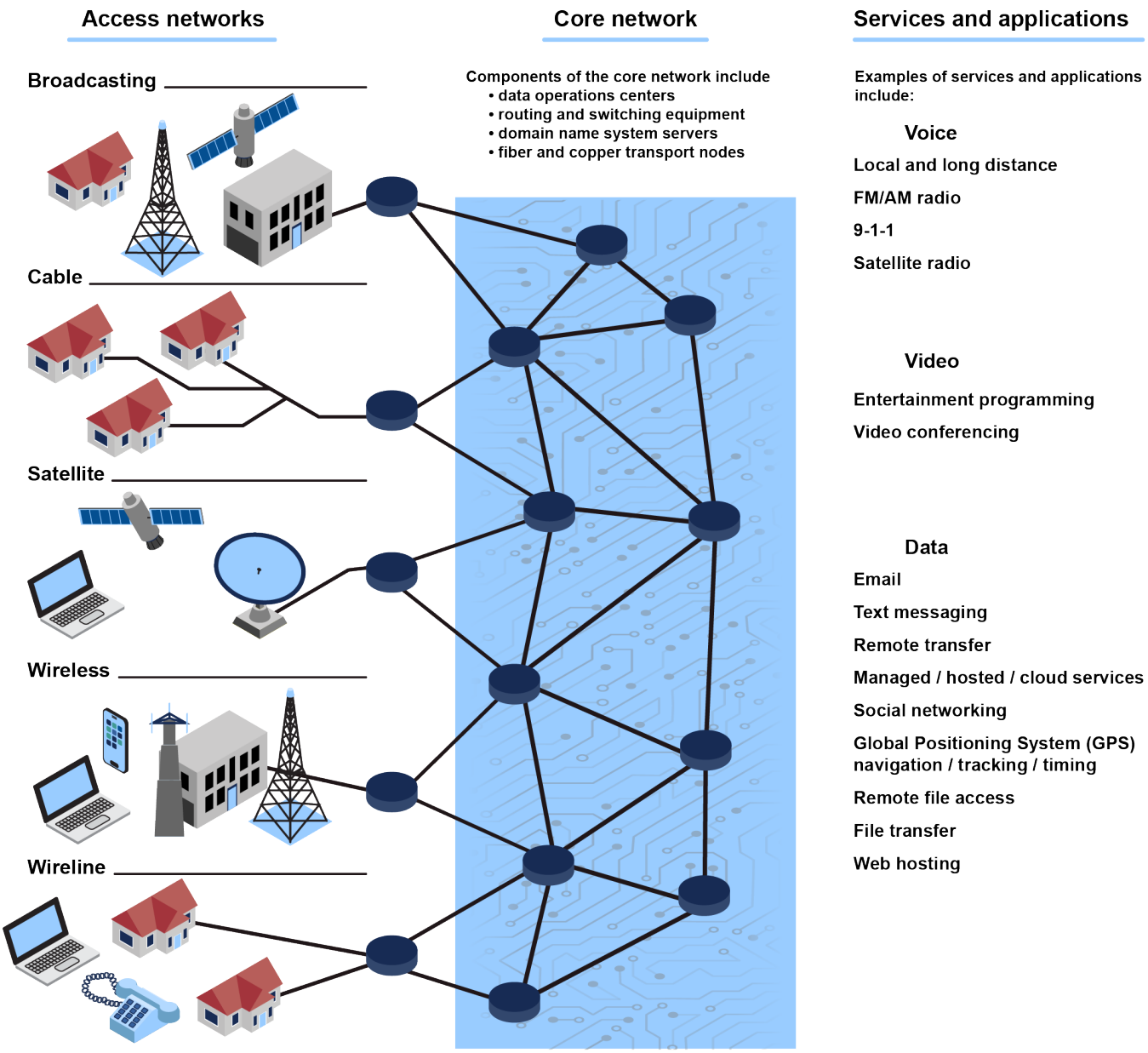
The key components of the systems and technology across all five industry segments include core networks, access networks, and services and applications (e.g., cell phones, computers, and webhosting).

- Core networks transport a high volume of aggregated multimedia (voice, data, and video) traffic combined from different service providers to be transported at high speed over substantial distances or between different service providers. These networks connect regions within the United States, as well as all continents except Antarctica, and use submarine fiber optic cable systems, land-based fiber and copper networks, and satellites. In order for the various Communications Sector segments (i.e., broadcast, satellite, wireless) to transmit data, service providers manage and control core infrastructure elements with numerous components, including signaling systems, databases, switches, routers, and operations centers.
- Access networks are primarily local portions of the communications network that connect end users to the core networks or directly to

each other and enable them to use services such as local and long distance phone calling, video conferencing, text messaging, e-mail, and various internet-based services. These services are provided by various technologies, such as satellites, wireless, cable, and wireline systems and assets.

- Communications services and applications include items such as satellite radio, video conferencing, and data cloud services that use core and access networks to send information and connect users with one another. As more devices, such as smartphones and tablet computers, connect to public communications networks, service firms can provide more types of device-specific services and applications over their networks. See figure 1 for an illustration of key Communications Sector systems and technology.

Figure 1: Key Components of the Communications Sector's Systems and Technology



Source: GAO analysis of Department of Homeland Security information. | GAO-22-104462

Note: Core communications networks transport a high volume of aggregated traffic—normally, the multimedia (voice, data, and video) traffic combined from different service providers to be transported over high speed through the core networks—over substantial distances or between different service providers. Core infrastructure systems and technology include signaling systems, databases,

switches, routers, and operations centers. Access communications networks are primarily local portions of the network that connect end users to the core communications network, or directly to each other, and enable them to use services such as local and long distance phone calling, video conferencing, and text messaging.

Federal Critical Infrastructure Policies and Plans

DHS's 2013 *National Infrastructure Protection Plan* (National Plan) is to guide the national effort to manage risk to the nation's critical infrastructure.[15] According to the National Plan, voluntary collaboration among private sector owners and operators and their government counterparts has been and will remain essential for national critical infrastructure security and resilience. The National Plan includes the *Critical Infrastructure Risk Management Framework*, which describes the activities that critical infrastructure partners are to collaboratively undertake to inform decision-making on actions intended to address identified infrastructure and related risks.[16] As part of the National Plan, in 2015, DHS issued the *Communications Sector-Specific Plan* to guide voluntary, collaborative efforts to improve security and resilience efforts, inform partner decisions, and improve risk management practices in the sector.[17]

In addition, DHS's *2019 National Response Framework* (Framework) is to guide how the nation responds to all types of disasters and emergencies.[18] The Framework includes Emergency Support Functions, which are key response-coordinating structures at the federal level. Specifically, the Framework identified 15 such functions—such as communications, transportation, and energy—and designated a federal department or agency as the coordinating agency for each function. CISA is designated as the federal coordinator for Emergency Support Function #2, which supports government and industry efforts to (1) restore critical communications infrastructure and services during incidents (e.g., hurricanes and wildfires), (2) facilitate the stabilization of systems and applications from malicious activity (e.g., cyber), and (3) coordinate communications support to response efforts such as emergency alerts

[15]Department of Homeland Security, *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience.*

[16]The *Critical Infrastructure Risk Management Framework* includes the following activities: (1) set goals and objectives; (2) identify infrastructure; (3) assess and analyze risks; (4) implement risk management activities; and (5) measure effectiveness.

[17]Department of Homeland Security*, Communications Sector-Specific Plan - An Annex to the National Infrastructure Protection Plan 2013*.

[18]Department of Homeland Security, *National Response Framework*, 4th ed.

and telecommunications. CISA, as the federal coordinator for Emergency Support #2, is responsible for management oversight throughout the preparedness, response, and recovery phases of incident management. In addition to the federal coordinator, each Emergency Support Function is composed of a number of primary and support agencies. Primary agencies are designated on the basis of their authorities, resources, and capabilities. Support agencies are assigned based on resources or capabilities in a given functional area.

In January 2021, the National Defense Authorization Act for Fiscal Year 2021 established sector risk management agency responsibilities for federal departments or agencies designated as such for each critical infrastructure sector or subsector.[19] These responsibilities include risk and vulnerability assessment activities, supporting incident management and restoration efforts, facilitating information sharing, contributing to emergency preparedness planning and exercises, and serving as a day-to-day federal interface for the prioritization and coordination of sector-specific activities.

Communications Sector Stakeholder Roles and Responsibilities

CISA is the designated lead agency, or sector risk management agency, responsible for coordinating efforts to help protect and improve the security and resilience of the Communications Sector.[20] To fulfill its sector risk management agency responsibilities, CISA works with a variety of entities, including the following:

- The Federal Communications Commission regulates interstate and international communications by radio, television, wire, satellite, and cable throughout the United States. The Federal Communications Commission also determines spectrum allocation and licensing matters for nonfederal users.[21] The Federal Communications

[19]See Pub. L. No. 116-283, § 9002(c).

[20]In addition to the Communications Sector, CISA is also the designated sector risk management agency for the following critical infrastructure sectors: Chemical; Commercial Facilities; Critical Manufacturing; Dams; Emergency Services; Information Technology; and Nuclear Reactors, Materials, and Waste.

[21]Spectrum is the range of all frequencies of electromagnetic radiation that are subdivided into frequency bands used by a wide variety of technologies, including communications technology, to operate. For recent work on the Federal Communications Commission's management of spectrum use, see GAO, *5G Deployment: FCC Needs Comprehensive Strategic Planning to Guide Its Efforts*, GAO-20-468 (Washington, D.C.: June 12, 2020); and *Internet of Things: FCC Should Track Growth to Ensure Sufficient Spectrum Remains Available*, GAO-18-71 (Washington, D.C.: Nov. 16, 2017).

Commission is also designated as a support agency for Emergency Support Function #2.[22]

- The National Telecommunications and Information Administration, within the Department of Commerce, is the principal presidential adviser on telecommunications and information policies and manages the federal government's use of spectrum.[23] The National Telecommunications and Information Administration is also designated as a support agency for Emergency Support Function #2.
- FEMA is the lead federal agency within DHS responsible for disaster preparedness, response, and recovery. FEMA is also designated as a primary agency specifically for Emergency Support Function #2, with responsibilities such as managing mission assignments—orders that FEMA issues to other federal agencies—and coordinating with other federal agencies, state officials, operations centers, and stakeholders during Stafford Act incidents.[24]
- The Communications Sector Coordinating Council is a private industry-led group that helps to coordinate key initiatives such as improving the physical and cyber security of Communications Sector assets; easing the flow of information within the sector, across sectors, and with designated federal agencies; and addressing issues related to response and recovery following an incident or event.

[22]In April 2021, we reported on the need for DHS to further clarify the Federal Communications Commission's Emergency Support Function #2 roles and responsibilities. As of September 2021, DHS was in the process of updating Emergency Support Function #2 to list specific roles and responsibilities for the Federal Communications Commission, in response to our recommendation. See GAO, *Telecommunications: FCC Assisted in Hurricane Maria Network Restoration, but a Clarified Disaster Response Role and Enhanced Communication Are Needed*, GAO-21-297 (Washington, D.C.: Apr. 29, 2021).

[23]For additional information on the National Telecommunications and Information Administration's spectrum management role, see GAO, *Spectrum Management: Agencies Should Strengthen Collaborative Mechanisms and Processes to Address Potential Interference*, GAO-21-474 (Washington, D.C.: June 29, 2021).

[24]In accordance with the Stafford Disaster Relief and Emergency Assistance Act (Stafford Act), as amended, the President may declare that a major disaster exists. 42 U.S.C. § 5170. The Stafford Act defines a "major disaster" as any natural catastrophe or, regardless of cause, any event in any part of the United States that the President determines causes damage of sufficient severity and magnitude to warrant major disaster assistance to supplement the efforts and available resources of states, local governments, and disaster relief organizations. See 42 U.S.C. § 5122(2). FEMA has multiple mechanisms to coordinate and implement federal disaster response and recovery activities, such as requesting that other federal agencies use their resources and authorities granted to them under federal law in support of direct assistance to disaster-affected locations.

- The Communications Sector Government Coordinating Council, a government-led group, chaired by CISA, acts as the counterpart and partner to the Communications Sector Coordinating Council to provide interagency, intergovernmental, and cross-jurisdictional coordination activities. The council also helps plan, prioritize, coordinate, implement, and execute sector-wide cybersecurity, infrastructure security, and resilience efforts. The Federal Communications Commission and the National Telecommunications Information Administration are also members of the Communications Sector Government Coordinating Council.
- The Communications Information Sharing and Analysis Center is a private sector-led organization formed by owners and operators to facilitate the exchange of information among industry and government participants regarding vulnerabilities, threats, intrusions, and anomalies affecting the telecommunications infrastructure. The center works with the National Coordinating Center for Communications—a joint industry/government center within CISA—to assist in the initiation, coordination, restoration, and reconstitution of national security and emergency preparedness communications services or facilities under all conditions of emerging threats, crisis, or emergency.

CISA Has Identified Physical, Cyber-related, and Human Threats to the Communications Sector

The Communications Sector faces serious physical, cyber-related, and human threats that could affect operations of local, regional, and national level networks, according to DHS's *2012 Risk Assessment Report for Communications*.[25] According to CISA officials, CISA uses these threat categories as a basis for developing and evaluating mitigation measures for the sector. In addition, the Communications Sector depends on five other critical infrastructure sectors for continued operations, as described below. CISA considers the dependence on other critical infrastructure sectors as a potential threat to the Communications Sector.

[25]In 2012, the Department of Homeland Security's National Communications System (which previously served as the sector specific agency for the Communicators Sector, a role now assigned to DHS's CISA) conducted a comprehensive assessment, with participation by sector stakeholders, to identify threats to the Communications Sector. According to CISA officials and sector stakeholders we interviewed, this assessment describes continuing and relevant threats to the Communications Sector. Local threats are Communications Sector component threats that affect the operation of a network in a local area, such as a metropolitan statistical area or micropolitan statistical area. A regional threat is a local threat that affects multiple states. A national threat affects the operation of a network on a national scale; they are events involving multiple FEMA regions.

Physical Threats

Physical Threats to Communications Infrastructure and Damage Caused by Hurricane Maria

In 2017, Hurricane Maria severely damaged communications-critical infrastructure in Puerto Rico and in the U.S. Virgin Islands. At the worst point following Hurricane Maria, 96 percent of telecommunications cell sites—equipment needed to receive and transmit radio signals for cellular voice and data transmission—were out of service in Puerto Rico, and 77 percent were out in the U.S. Virgin Islands. This outage left residents without reliable and continuous access to voice and data communications. Without telecommunication services, people were unable to call for help during a medical emergency or to receive mobile weather alerts on floods and landslides.

Source: GAO. | GAO-22-104462

The physical threats to the Communications Sector include threats from natural occurrences (e.g., ice storms, urban floods, and earthquakes) and human-made events (e.g., intentional electromagnetic interference, explosives, or submarine cable damage). Events from physical threats can cause severe damage to communications infrastructure—such as buildings, electric substations, microwave and satellite antennas, fiber optic amplifiers, and hybrid fiber-coaxial systems—potentially resulting in communications disruptions across the sector. See table 2 for additional details on physical threats to the Communications Sector identified by DHS.

Table 2: Physical Threats and Potential Impacts to the Communications Sector Identified by the Department of Homeland Security (DHS)

Physical threats	Threat description and potential impact
Naturally occurring physical threats	
Category 4 or 5 hurricane	Hurricanes generate winds that can damage utility poles, aerial infrastructure, and other communications equipment. The resulting damage and power outages may also limit recovery efforts.
Tornado	Tornadoes produce winds that can damage buildings, aerial lines and cables, as well as other infrastructure.
Major urban flood	Floods have the potential to expose and damage buried cables and other communications equipment. Floodwaters and debris can also impede restoration of communications services.
Rural wildfire	Wildfires can damage electric transmission and distribution systems, as well as wooden poles and aerial equipment, including fiber optic and copper lines, microwave towers, and equipment in vaults. Smoke from wildfires may be drawn in to communications buildings through ventilation systems, which could require heating, ventilation, and air conditioning to be temporarily shut down.
Urban snow and ice storm	Urban snow and ice storms primarily affect aerial cables by causing trees to collapse on the cables or by overstressing the cables. Damaged cables can lead to local communications disruptions and power outages, and unplowed roads can impede recovery efforts.

Physical threats	Threat description and potential impact
Solar storm	Solar storms are a naturally occurring phenomenon in which the sun releases solar flares, energetic particles, or coronal mass ejections.[a] Solar storms can interact with the Earth's magnetic field, cause geomagnetic storms, and induce geomagnetically-induced currents in the ground, which can impact communications and electrical equipment, such as extra- high-voltage transformers. Solar storms can also damage satellites and disrupt Global Positioning System capabilities.
Major earthquake	A major earthquake involves the violent and sudden release of energy in the Earth's crust. The ensuing seismic waves can substantially damage structures, utility poles, and underground infrastructure.
Human-caused physical threats	
Intentional electromagnetic interference attack	Intentional malicious generation of electromagnetic energy that produces currents and voltage surges that disrupt or damage communications equipment and systems for terrorist or criminal purposes.
Chemical, biological, or radiological contaminant attack	An attack that introduces a human disease, generates poison gases or other chemical hazards, or produces radiation resulting in contamination or casualties. Contamination may kill communications personnel or render an area inaccessible, thereby preventing equipment from being maintained or repaired.
Explosives attack	A terrorist attack using a large amount of explosives or improvised explosive devices, airborne improvised explosive devices, and vehicle-borne improvised explosive devices can damage buildings and facilities housing communications infrastructure, killing personnel or rendering an area inaccessible.
High-altitude electromagnetic pulse attack	A large-scale electromagnetic pulse can be produced by a single nuclear explosion detonated high in the atmosphere. High-altitude electromagnetic pulse attacks are capable of short-circuiting a wide range of electronic equipment, particularly computers, satellites, and radios. Low earth orbit satellites operate in the range of the inner radiation belt and, therefore, are susceptible to a high-altitude electromagnetic pulse attacks.
Source region electromagnetic pulse attack	An electromagnetic pulse attack can occur after a small nuclear device detonates at ground level. These attacks induce large electric currents in conductors such as power lines and communications cables within and outside of buildings. These attacks are likely to damage communications infrastructure such as ethernet-based data systems.
System-generated electromagnetic pulse	A system-generated electromagnetic pulse attack occurs when an antisatellite weapon above the Earth unleashes gamma and x-rays from a high-altitude detonation. When this radiation strikes a satellite, it damages the satellite and may make it inoperable.
Submarine cable damage[b]	Submarine cables are most frequently unintentionally damaged in shallow waters near the shore from accidents involving driftnets, ship anchors, or dredging equipment. However, naturally occurring threats, such as earthquakes, can damage submarine cables. Malicious actors also pose a threat to submarine cables and can exploit cybersecurity vulnerabilities at submarine cable landing sites (i.e., locations where submarine cables connect to land-based networks) or cause intentional damage.

Source: GAO analysis of DHS documentation. | GAO-22-104462

[a]Coronal mass ejections are large expulsions of plasma and magnetic field from the sun's corona.

[b]Submarine cables provide the primary means of connectivity—voice, data, and internet—between the United States and the rest of the world, as well as connectivity between the mainland United States and consumers in Alaska, Hawaii, Guam, American Samoa, the Northern Mariana Islands, Puerto Rico, and the U.S. Virgin Islands.

Cyber-related Threats

Cyber-related Threats from Botnets

A botnet is a network of internet-connected end-user computing devices infected with bot malware and that are remotely controlled by third parties for nefarious purposes. A botnet attack happens when a network of computers, Internet of Things, or other internet protocol-enabled devices are commandeered to run unauthorized code in support of malicious activities such as spam, phishing, click-fraud, and distributed denial of service.

In March 2021, the Department of Homeland Security's Cyber Security and Infrastructure Security Agency and the Federal Bureau of Investigation released an advisory on TrickBot malware, which is used to attack individuals and businesses.

Sources: Department of Homeland Security and the Federal Bureau of Investigation. | GAO-22-104462

The cyber-related threats to the Communications Sector include threats from both malicious actors (e.g., adversaries who intentionally cause network disruptions) and nonmalicious actors (e.g., employees that accidently cause network disruptions). For example, a malicious actor could intentionally affect software or exploit security gaps in an effort to change or disrupt the systems on a communications network, potentially making the data managed on the network or systems unreliable. Alternatively, a nonmalicious actor (e.g., a vendor) could accidentally alter a communication network's configuration, negatively affecting the network's ability to function properly. According to DHS, most cyber-related threats, if realized, can lead to communications disruptions that impact only local or regional areas. This is because many service providers already deploy capabilities to automatically reroute data traffic to minimize the impact of a network failure from a cyberattack. In addition, communications networks are designed to sustain availability by leveraging interconnections between providers' networks. However, in its 2012 risk assessment report, DHS reported that a cyber-related attack on a Communications Sector's network could temporarily prevent a company from sending and receiving information on all of its network's interfaces, or it could exploit security gaps in a network to steal confidential information. See table 3 for additional details on cyber-related threats to the Communications Sector identified by DHS.

Table 3: Cyber-related Threats and Potential Impacts to the Communications Sector Identified by the Department of Homeland Security (DHS)

Cyber-related threats	Threat description and potential impact
Malicious actor—resource exhaustion	A malicious actor tries to overwhelm the resources of hardware, software, or network capacity (e.g., denial of service attack, botnet, worm, etc.).[a] A malicious actor could exploit or alter firmware embedded on a device.
Malicious actor—system alteration	A malicious actor could exploit or alter firmware, application, hardware, or security gaps to alter systems, thus making the managed data unreliable.
Malicious actor—system intrusion	A malicious actor could gain unauthorized access to sensitive information within the network and exploit or alter firmware, application, hardware, or security gaps to gain access to internal systems and steal confidential information.
Malicious actor—white space database attack	The conversion of television and radio stations from analog to digital transmission in 2009 freed white space frequencies that will be managed in a database to prevent interference.[b] In this scenario, an attack is launched to disrupt the database, thereby disrupting frequency tracking and affecting broadcasting.
Nonmalicious actor—resource exhaustion	An employee could install a software patch without properly testing it prior to implementation, causing a company to exhaust resources. The accidental installation of bad firmware, applications, or hardware can also cause a company to exhaust resources.
Nonmalicious actor—system alteration	System alterations could occur when a person, program, or vendor accidentally alters the network configuration whose effects are not fully known and triggers a series of actions, leading to data changes.

Cyber-related threats	Threat description and potential impact
Nonmalicious actor—other accident	An accident not included under system alteration or resource exhaustion; for example, accidentally plugging a cable into the wrong port. A software upgrade, failure to download a software upgrade, or purchasing the wrong equipment could also result in system malfunctions.
Nonmalicious actor—white space database event	An event is accidentally launched to disrupt the database, thereby disrupting frequency tracking and affecting broadcasting. The software to manage the database could become disrupted during an upgrade, or the wrong equipment could be purchased, leading to interference.

Source: GAO analysis of DHS documentation. | GAO-22-104462

[a]A worm is an independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to manifest.

[b]TV white space is unlicensed spectrum from unused channels in the broadcast television spectrum band.

Human Threats

Training Employees to Defend Against Human Threats and Detect Threats Caused by Foreign Malicious Actors

In 2021, the Cybersecurity and Infrastructure Security Agency (CISA) identified a threat posed to telecommunication firms and other critical infrastructure sectors by Chinese state-sponsored cyber actors. These threat actors were aggressively targeting U.S. critical infrastructure sectors to steal sensitive data, intellectual property, and other important information.

As a result, CISA issued a notice to critical infrastructure sector owners and operators, such as telecommunications companies, to ensure that personnel are familiar with the key steps to take during an incident. In its notice, CISA urged telecommunications personnel to monitor key internal security capabilities and to be prepared to identify anomalous behavior and know how and when to report an incident. CISA also urged critical infrastructure partners to train employees to ensure that they have the ability to flag any known Chinese state-sponsored indicators of compromise and tactics, techniques, and procedures for immediate response.

Source: CISA. | GAO-22-104462

The human threats to the Communications Sector include threats to a communications network created due to the failure of employees taking action to plan for security incidents and implementing protocols to protect networks from the impacts of such incidents. For example, a human threat is created when employees fail to develop access management plans prior to a disaster. Access management plans outline details such as which communications personnel and vehicles should be cleared to enter disaster sites, who will carry out response and recovery duties, or the type and amount of personal protective equipment employees may need prior to entering a disaster site. Human threats are also created when employees lack security awareness or are not trained to detect possible threats. For example, employees who do not receive adequate security awareness training, or do not have information technology backgrounds, may have difficulty identifying an attempted breach. Employees may also attempt to address an information technology issue that they are neither capable of addressing, nor authorized to address, rather than reporting incidents to their information technology departments. Without thorough employee training, networks may be vulnerable to threat actors that exploit a lack of employee security awareness. According to DHS, most of the human threat impacts would be limited to local or regional areas and would not result in national communications disruptions or outages. See table 4 for additional details on human threats to the Communications Sector identified by DHS.

Table 4: Human Threats and Potential Impacts to the Communications Sector Identified by the Department of Homeland Security (DHS)

Human threats	Threat description and potential impact
Lack of access management plans	After a disaster or a mass communications outage, preventing communications personnel from entering the affected site could affect the security and resilience of the communications network and delay recovery time. Communications personnel are often restricted from accessing disaster areas to complete response and recovery duties when access management plans are not in place and personnel are not properly cleared for access (pre-event access planning issue) or when plans are in place but are improperly followed (post-event access management issue).
Lack of security and equipment during response and recovery	Communications Sector recovery efforts can be delayed when personnel are not provided with police or private security protection, personal protective equipment, secure areas for vehicles and communications equipment, and cooperation from local jurisdictions controlling access to disaster areas.
Lack of employee security awareness	When Communications Sector employees are unaware of security policies and procedures, security threats can occur. Without thorough employee training, employee workstations, network infrastructure, or corporate enterprise infrastructure may be vulnerable to malicious actors that exploit a lack of employee security awareness.
Internal threats	Sensitive network operations equipment, databases, and systems operations are vulnerable as a result of improperly, or poorly managed, physical or logical security; missed identification of potential security issues; or misplaced trust in a single individual with system administrator privileges without adequate backup or oversight (e.g., recording of changes).
External threats	Communications networks are vulnerable as a result of insufficient security controls and insufficient protective measures against criminal activities (e.g., espionage, fraud, bribery, blackmail, or extortion); employee gullibility; insufficient awareness of security policies; and inadequate employee screening, training, and behavior monitoring.

Source: GAO analysis of DHS documentation. | GAO-22-104462

Communications Critical Infrastructure Sector Dependencies

Communications Sector Dependence on the Energy Sector

In 2018, the President's National Infrastructure Advisory Council highlighted the Communications Sector's reliance on the Energy Sector (e.g., fuel to operate generators, and transporting fuel from pipeline pumping stations). Likewise, disaster restoration and recovery are next to impossible without working communications.

For example, in 2017, Hurricane Maria severely damaged telecommunications networks in Puerto Rico and in the U.S. Virgin Islands. The lack of electrical power was the most noteworthy challenge in restoring communication networks. Restoration crews did not have electricity to conduct accurate damage assessments of communications networks to report on available services and check signal reception. Furthermore, without power, the carriers relied on back-up generators to operate network equipment for months, 7 days a week. The necessary fuel for these generators and trucks for telecommunications crews was scarce, and theft of both fuel and generators further complicated the carriers' restoration efforts

Sources: GAO and President's National Infrastructure Advisory Council, *Surviving a Catastrophic Power Outage: How to Strengthen the Capabilities of the Nation* (December 2018). | GAO-22-104462

In addition to the three threat categories described above, DHS also identified disruptions to other critical infrastructure sectors as a threat to the security and resilience of the Communications Sector. According to DHS's 2012 risk assessment report, these sectors are so closely connected and interdependent that damage, disruption, or destruction to one infrastructure element in one sector can cause cascading effects, potentially affecting the continued operation of the Communications Sector.

According to DHS, the Communications Sector depends on five other critical infrastructure sectors to ensure continued operation: (1) the Defense Industrial Base (specifically, Global Positioning System (GPS) technology), (2) Energy, (3) Information Technology, (4) Transportation Systems, and (5) Water and Wastewater Systems. See table 5 for more information on these dependencies.

Table 5: Communications Sector Critical Dependencies Identified by the Department of Homeland Security (DHS)

Critical dependencies	Threat description and potential impact
Defense Industrial Base Sector (Global Positioning System (GPS) specific technologies)	The U.S. Air Force owns and operates the country's GPS satellite constellation. GPS supports a broad range of Communications Sector functions and applications. The primary use for GPS services is to support networks' precise timing and synchronization requirements. As such, a long-term disruption of GPS technologies could reduce the accuracy of communications networks. For example, the loss of GPS capabilities would affect the ability to determine accurate location information for wireless E911 purposes.[a]
Energy Sector	Many communications networks depend on commercial electric power in order to function. Although Communications Sector infrastructure can use backup electric power systems to keep its critical network components operational in the event of an electric power outage, backup systems may not be designed to operate long term, due to the cost of building and maintaining large diesel generators, as well as the difficulty of storing more than a few days of fuel on-site.

Critical dependencies	Threat description and potential impact
Information Technology Sector	The Information Technology Sector produces several key products and services used by the Communications Sector, such as software systems; managed network/data center elements; semiconductors; and storage hardware. Loss of access to this sector's products and services would have a substantial impact on the Communications Sector.
Transportation Sector	During long-term power outages (i.e., 96 hours or longer), the security and resilience of the Communications Sector depends on the sector's ability to partner with Transportation Sector components (i.e., trucks carrying fuel, and fuel pumping stations) to deliver fuel for generators. If the delivery of fuel is impeded during a long-term outage, threats to security and resilience are compounded and may result in prolonged outages.
Water Sector	The Water Sector provides potable water to many commercial facilities that house elements of the Communications Sector. Communications Sector components rely on having access to clean sources of water for heating and cooling. For example, data centers use high-tonnage heating ventilation and air conditioning systems to operate and to keep their computer systems cool. While communications service providers generally have alternate sources of water available for short-term service interruptions, a long-term outage could result in a significant shutdown of the Communications Sector.

Source: GAO analysis of DHS documentation. | GAO-22-104462

[a]E911 (Enhanced 911) is a service that automatically displays the telephone number and location information for wireless 911 calls on the emergency operator's screen.

CISA Supports the Security and Resilience of the Communications Sector through Incident Management and Information-Sharing

CISA primarily supports the Communications Sector through incident management and information-sharing activities. CISA also supports the Communications Sector, and other critical infrastructure sectors, through other programs and services, such as cybersecurity programs; strategic initiatives; educational materials; and services provided by CISA field personnel. In addition, CISA employs an all-hazards approach to work with private sector and government stakeholders to prepare for, mitigate, respond to, and recover from a variety of natural (i.e., floods and tornados) and human-caused (i.e., chemical or explosive attack) incidents. According to DHS's *Communications Sector-Specific Plan*, voluntary collaboration between private sector and government stakeholders remains the primary mechanism for advancing sector security and resilience.

Incident management. In its capacity as the federal coordinator for Emergency Support Function #2, CISA is responsible for coordinating federal activities to support Communications Sector infrastructure owners and operators during incidents such as outages caused by severe

weather.[26] The purpose of Emergency Support Function #2 is to support restoration of communications infrastructure, facilitate the recovery of systems and applications from cyberattacks, and coordinate federal communications support during incidents requiring a coordinated federal response. CISA officials stated that CISA's regional and headquarters personnel are the primary resources used to support the agency's Emergency Support Function #2 responsibilities.

In fulfilling these responsibilities, CISA primarily works with other federal agencies that have authorities, roles, resources, and capabilities within Emergency Support Function #2 to support response and restoration efforts.[27] For example, during Emergency Support Function #2 response efforts, CISA is to work with the Federal Communications Commission and the National Telecommunications and Information Administration to ensure spectrum availability for communication services, such as mobile voice and data that first responders and other entities may rely on during an incident. According to CISA officials, CISA does not typically provide equipment (e.g., generators) for restoration of communications infrastructure. Rather, these officials stated that other government agencies, such as FEMA, and private sector owners and operators, supply the majority of equipment. The officials added that Communications Sector owners and operators typically request assistance from CISA when they cannot handle an incident on their own, such as during a large-scale disruption or outage. For example, in February 2021, CISA, through Emergency Support Function #2, supported responses to severe winter weather in Texas that caused power and telecommunications services outages. According to CISA officials, activities to support recovery efforts included coordination to

[26]Emergency Support Functions are the federal government's primary coordinating structure for building, sustaining, and delivering response capabilities when a national response is needed. Not all incidents requiring federal support result in the activation of Emergency Support Functions. There are 15 Emergency Support Functions, each defining specific functional areas—such as communications, transportation, and energy—for the most frequently needed capabilities during an emergency to help coordinate the provision of assets and services by departments and agencies. CISA is also the federal coordinator for Emergency Support Function #14, which coordinates cross-sector operations with infrastructure owners and operators, businesses, and their government partners, with particular focus on actions taken by businesses and infrastructure owners and operators in one sector to assist other sectors to better prevent or mitigate cascading failures between them.

[27]Outside of coordinating federal response and recovery activities to an incident impacting the Communications Sector, CISA's activities also include weekly conference calls with Emergency Support Function #2 members, training workshops, and participation in national exercises.

provide communications infrastructure owners and operators with generators and diesel fuel to supply electrical power to communications infrastructure facilities.

CISA also coordinates federal activities to support sector infrastructure owners and operators outside of Emergency Support Function #2 activities. Incident response activities occur through CISA Central, which is a single operations center integrating cyber, physical, and communications activities to coordinate situational awareness and response to cyber, communications, and physical incidents of national importance. For example, on December 25, 2020, a bomb detonated from inside a vehicle parked in downtown Nashville, Tennessee. The explosion damaged more than 40 buildings, knocked out commercial power, and destroyed the power infrastructure that linked to the fixed backup generators for the facility housing communications critical infrastructure. CISA officials stated that they coordinated with law enforcement to provide company officials with access to the damaged building to support recovery efforts, and full restoration of services occurred within a few days.

Information-sharing activities. In addition to managing federal coordination during incidents impacting the Communications Sector, CISA shares information with sector stakeholders to enhance their cybersecurity and improve interoperability, situational awareness, and preparedness for responding to and managing incidents. CISA primarily shares information with Communications Sector stakeholders through the National Coordinating Center for Communications, which is part of CISA Central, and the Communications Information Sharing and Analysis Center, which is private sector-led and consists of approximately 80 members.[28] According to CISA officials, the centers exchange open source, protected, and classified information that can inform actions to protect and preserve communications infrastructure. Examples of information shared by the centers include current cybersecurity advisories and reports on the impact of hurricanes on critical infrastructure sectors.

Other programs and services. CISA also supports critical infrastructure sectors, including the Communications Sector, through cybersecurity

[28]In general, sector-specific information-sharing and analysis centers are nonprofit, member-driven organizations formed by critical infrastructure owners and operators to share information between government and industry.

programs, strategic initiatives, educational materials, and other services provided by CISA field personnel.

- **Cybersecurity programs:** According to CISA officials, Communications Sector stakeholders participate in its cybersecurity programs, which provide participants with information about cybersecurity threats and methods to mitigate them.[29]
- **Strategic initiatives.** CISA participates in a variety of strategic initiatives to identify and address new and emerging threats and risks to critical infrastructure sectors, including the Communications Sector. These initiatives began at the direction of executive orders and involve topics such as information and communications technology to support supply chain security, as well as position, navigation, and timing (PNT) technology and services.[30] Further, these initiatives include participation by the Departments of Homeland Security, Commerce, Transportation, and Defense and the Federal Communications Commission, among others. Through the initiatives, CISA has also released a variety of products to support security and resilience, including those that identified risks and threats to the Communications Sector. For an overview of these initiatives, see table 6 below.

[29]According to CISA officials, those cybersecurity programs include the Automated Indicator Sharing, Enhanced Cybersecurity Services, and Cyber Information Sharing and Collaboration programs. The Automated Indicator Sharing program enables the real-time exchange of machine-readable information to help protect against cyberattacks. The Enhanced Cybersecurity Services program allows for sharing of unclassified and classified information on malicious cyber activity. The Cyber Information Sharing and Collaboration Program includes sharing information on cybersecurity threats with critical infrastructure sectors through reports and bulletins.

[30]See Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services, Exec. Order No. 13905, 85 Fed. Reg. 9359 (Feb. 18, 2020) (issued Feb. 12); Securing the Information and Communications Technology and Services Supply Chain, Exec. Order No. 13873, 84 Fed. Reg. 22689 (May 17, 2020)(issued May 15); and Coordinating National Resilience to Electromagnetic Pulses, Exec. Order No. 13865, 84 Fed. Reg. 12041 (Mar. 29, 2019) (issued Mar. 26). The Information and Communications Technology Supply Chain Risk Management Task Force was chartered under the Critical Infrastructure Partnership Advisory Council, which facilitates interactions between governmental entities and representatives from the community of critical infrastructure owners and operators.

Table 6: Department of Homeland Security (DHS) Communications Sector Strategic Initiatives

Initiative	Description and overview
Information and communication technology (ICT) supply chain risk management (SCRM)	Initiative description: ICT SCRM is the process of identifying, assessing, and mitigating the risks associated with the global and distributed nature of ICT products and services—e.g., computing systems, software, and networks—supply chains. Overview: In 2018, the Cybersecurity and Infrastructure Security Agency (CISA) within DHS established the ICT SCRM Task Force—a public-private partnership focused on global ICT supply chain security. The objectives of the ICT SCRM Task Force are to (1) act as a forum for collaboration with private sector critical infrastructure owners and operators on methods and practices to effectively identify, prioritize, and mitigate ICT supply chain risks; (2) provide realistic, actionable, timely, economically feasible, scalable, and risk-based recommendations for addressing ICT supply chain risks; and (3) recommend methods for the development and implementation of improvements in risk management in global ICT supply chains. Through the ICT SCRM Task Force, CISA has released products to support efforts to address supply security threats and risks within the Communications Sector.
Fifth generation (5G) technology and security	Initiative description: 5G networks are the latest generation of mobile communications and are expected to provide faster connections to support consumer, industry, and public sector services. Overview: CISA is working with interagency and industry partners to mitigate risks and increase the security and resilience of 5G connectivity. For example, CISA has released a variety of products to inform critical infrastructure owners and operators on risks associated with the deployment and use of 5G technology, including its 2020 5G strategy that establishes initiatives to advance the deployment of a secure and resilient 5G infrastructure. The strategy notes that each of the initiatives should address critical risks to secure 5G deployment, such as physical security concerns; attempts by threat actors to influence the design and architecture of the network; and vulnerabilities within the 5G supply chain.
Position, navigation, and timing (PNT) technology and services	Initiative description: PNT services are any system, network, or capability that provides a reference to calculate or augment the calculation of longitude, latitude, altitude, or transmission of time or frequency data. Overview: DHS, through CISA, is taking actions to address risk associated with use of PNT technology and services. CISA has released products with information on threats and vulnerabilities associated with the use of PNT technology and services. For example, in April 2020 CISA, along with the Department of Transportation, released a report on civilian backup PNT capabilities to the Global Positioning System.
Electromagnetic pulse (EMP) attack and naturally occurring geomagnetic disturbance (GMD)	Initiative description: An electromagnetic event can result from a naturally occurring, large-scale GMD, caused by severe solar weather. An electromagnetic event can also result from human-made sources, such as nonnuclear EMP weapons—those that produce electromagnetic radiation, such as devices that generate localized EMP using microwave-type technologies. Overview: DHS, through CISA and in coordination with interagency partners, is taking actions—including vulnerability assessments, testing, and private sector coordination, among others—to address EMP-related vulnerabilities to critical infrastructure. DHS, including work completed by CISA, has released products identifying risks and vulnerabilities associated with EMP and GMD, including to the Communications Sector.

Source: DHS information. | GAO-22-104462

- **Educational materials and services.** CISA offers a variety of educational materials and services to critical infrastructure owners and operators. CISA's products and services include risk management and response services to build stakeholder resiliency and to form partnerships. Examples of such services and products include webinars and other training, tabletop exercises, and technical assistance and tools. In particular, CISA provides guides and webinars to help individuals and organizations prevent ransomware attacks that can severely impact business processes and leave organizations without the data they need to operate and deliver mission-critical services.[31]
- **Field support services.** CISA provides support services to federal, state, local, tribal, and territorial government mission partners and Communications Sector owners and operators through Protective Security Advisors and Cybersecurity Advisors, based in 10 regional offices.[32] These advisors support critical infrastructure owners and operators by providing products and services such as assessments, training, exercises, and workshops. For example, Protective Security Advisors complete surveys and assessments that help identify the security and resilience of individual owners' and operators' facilities. Cybersecurity Advisors, for example, provide briefings and assessments of cybersecurity and resilience for owners and operators.[33]

CISA Has Not Assessed Its Support to the Communications Sector nor Updated Its Sector Plan

[31]Ransomware is a type of malicious software designed to encrypt files on a device, rendering any files and the systems that rely on them unusable, whereby malicious actors then demand ransom in exchange for decryption.

[32]CISA's regional offices also include Emergency Communications Coordinators who support federal, state, local, tribal, and territorial government public safety communications mission partners.

[33]A Cyber Resilience Review assessment is a nontechnical assessment to evaluate an organization's operational resilience and cybersecurity practices.

CISA Has Not Assessed the Effectiveness of Its Actions to Support the Communications Sector

Although CISA has numerous programs and services to support the security and resilience of the Communications Sector, CISA has not assessed the effectiveness of these actions. Specifically, CISA has not assessed the effectiveness of its programs and activities used by sector owners and operators, including developing metrics and analyzing feedback received from owners and operators. According to CISA officials, CISA uses a variety of mechanisms to collect feedback from Communications Sector owners, operators, and other stakeholders, such as surveys, working groups, and formal meetings. However, CISA has not evaluated feedback it has received from Communications Sector owners and operators to determine if those entities found its programs and services useful or relevant. Further, CISA has not evaluated its programs and services to determine which types of Communications Sector owners and operators may benefit most from participation, such as large versus small telecommunications service providers. For example, a private sector organization we met with stated that small companies are often underrepresented participants in CISA's support activities due to small companies' inability to devote resources to coordination and information-sharing activities.

DHS's *Critical Infrastructure Risk Management Framework* states that use of metrics and other evaluation procedures to measure progress and assess the effectiveness of efforts to secure and strengthen the resilience of critical infrastructure informs the process of prioritizing and selecting the most effective and cost-efficient ways to manage risk.[34] According to DHS's *Critical Infrastructure Risk Management Framework*, assessing effectiveness could include developing metrics to indicate the effectiveness of security and resilience activities and the extent to which these activities are reducing risks.[35]

CISA officials told us that they have not assessed the effectiveness of actions to support the Communications Sector due to challenges in developing metrics to measure the effectiveness of its actions, including collecting voluntary information from sector owners and operators. As mentioned previously, CISA uses a variety of mechanisms to collect feedback from Communications Sector owners, operators, and other stakeholders on its programs and services. For example, according to

[34]Department of Homeland Security, *Supplemental Tool: Executing A Critical Infrastructure Risk Management Approach*.

[35]Department of Homeland Security, *Supplemental Tool: Executing A Critical Infrastructure Risk Management Approach*.

CISA officials, the agency sent surveys to owners and operators seeking feedback on assessments conducted by Physical Security Advisors, and actions taken in response to those assessments. CISA's mechanisms to collect feedback could serve as opportunities for CISA to collect any additional relevant information—such as which services and programs owners and operators find most beneficial for addressing threats—that would help CISA develop metrics to understand the effectiveness of its activities.

According to DHS's *2013 National Infrastructure Protection Plan*, owners and operators can support improvements by providing ongoing feedback on the needs and the application of information products by sharing information with the federal government.[36] By assessing the effectiveness of its programs and services to support the Communications Sector, to include developing and implementing metrics and analyzing feedback received from owners and operators, CISA would be better positioned to determine which activities are most useful or relevant in supporting the sector's security and resilience.

CISA Has Not Assessed Its Emergency Preparedness Capabilities for the Communications Sector

CISA has taken actions to support emergency preparedness for the Communications Sector, but has not completed an assessment of its capabilities to perform as the federal coordinator for Emergency Support Function #2. As the federal coordinator for Emergency Support Function #2, CISA is charged with supporting government and industry efforts to restore critical communications infrastructure and services during incidents such as hurricanes and wildfires. FEMA guidance on the activities and products needed to support Emergency Support Function preparedness calls for coordinator agencies, such as CISA, to conduct coordination activities, planning activities, and a capability assessment.[37]

Regarding coordination actions to support emergency preparedness, CISA has held weekly conference calls with Emergency Support Function #2 members, training workshops, and has participated in national exercises. During weekly conference calls, CISA meets with Emergency Support Function #2 private sector and government members and also participates in monthly FEMA-led Emergency Support Function Leadership Group meetings. The purpose of this leadership group is to

[36]Department of Homeland Security, *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience.*

[37]Department of Homeland Security, Federal Emergency Management Agency, *Memorandum for Emergency Support Function Leadership Group - Performance Metrics for Emergency Support Function Preparedness.*

provide a forum for departments and agencies with roles in federal incident response to jointly address matters pertaining to the community lifelines, emergency response policy, preparedness, operations, and training.

CISA's Emergency Support Function #2 planning activities include development of a concept of operations, a regional incident support manual, and a multiyear training and exercise plan. For example, the purpose of the multiyear training and exercise plan is to provide Emergency Support Function #2 stakeholders with an understanding of the desired skillsets and opportunities for planning, training, and exercise activities. The training plan includes objectives to train and educate Emergency Support Function #2 stakeholders on policies, procedures, and roles.

Although CISA has conducted coordination and planning activities to support Emergency Support Function #2 preparedness, it has not completed a capability assessment. According to the *National Response Framework*, response to emergencies and disasters will be most effective through capability-based planning. Capability-based planning can inform resource investment and allocation, drive deliberate planning efforts focused on the most challenging risks, and help government and private sector officials understand response and recovery capacities.[38] According to the *National Response Framework*, a capability assessment will also help identify where mutual aid or other assistance may fill capability gaps.

According to FEMA's 2015 Emergency Support Function guidance, a capability assessment may include establishing requirements for supporting the relevant Emergency Support Function, maintaining a list of resources needed to provide such support, and assessing existing capabilities against requirements to identify gaps for responding to incidents affecting the relevant critical infrastructure sector. In our prior work, we identified a few examples of capability assessment activities to support Emergency Support Functions.[39]

- Requirements could include, for example, agency staffing needed for Emergency Support Function operations during an incident.

[38]Department of Homeland Security, *National Response Framework*, 4th ed.

[39]GAO, *Emergency Preparedness: Opportunities Exist to Strengthen Interagency Assessments and Accountability for Closing Capability Gaps*, GAO-15-20 (Washington, D.C.: Dec. 9, 2015).

- A catalog of resources could include, for example, the type and quantity of resources available to each participating agency during Emergency Support Function operations during an incident.
- A capability gap analysis could determine whether participating agencies have sufficient resources to support Emergency Support Function operations during an incident.

CISA officials told us they have not completed any capability assessment activities for Emergency Support Function #2 due to challenges related to CISA's organizational transformation initiative and persistent Emergency Support Function #2 activities over the last 2 years.[40] As part of the organizational transformation initiative, in June 2020, CISA created a new group, the Emergency Support Function Coordination Group, responsible for the agency's incident management activities in support of Emergency Support Function #2. In addition to CISA's organizational transformation, it also faces a persistent workload from Emergency Support Function #2 activities supporting incident response and recovery efforts due to numerous severe weather events such as hurricanes. Recent incidents, such as Hurricane Ida in August 2021, continue to highlight the impact that severe weather can have on communications critical infrastructure and the importance of CISA's role as the federal coordinator for Emergency Function #2.[41] By assessing Emergency Support Function #2 capabilities, including understanding any capability gaps in staffing and resources, CISA will be better positioned to address challenges faced by persistent workloads and ensure preparedness for future incidents.

CISA Has Not Updated the *Communications Sector-Specific Plan*

According to DHS's 2013 National Plan, each critical infrastructure sector should update its sector-specific plan every 4 years to reflect priorities, address sector reliance on lifeline functions, describe national preparedness efforts, outline cybersecurity efforts, and develop metrics to measure progress on achieving sector goals.[42] To complete the 2015

[40]For more information on CISA's organizational transformation initiative, see GAO-21-236.

[41]According to the Federal Communications Commission's Communications Status Report for Areas Impacted by Hurricane Ida in August 2021, numerous areas in Louisiana experienced loss of wireless, wireline, and cable communications services. For example, about half of affected disaster areas in Louisiana lost wireless communications service.

[42]Department of Homeland Security, *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience.* Lifeline functions are those that are essential to the operation of most critical infrastructure sectors and include communications, energy, and transportation.

Communications Sector-Specific Plan, DHS undertook a process working with interagency partners and private sector stakeholders to revise the 2010 *Communications Sector-Specific Plan*.[43] Specifically, the 2015 *Communications Sector-Specific Plan* was developed as a collaborative effort among the private sector; state, local, tribal, and territorial governments; nongovernmental organizations; and federal departments and agencies to identify and work toward shared goals and priorities to reduce critical infrastructure risk. Further, the Communications Sector Coordinating Council and the Communications Sector Government Coordinating Council jointly developed the Communications Sector goals, objectives, and activities in the 2015 *Communications Sector-Specific Plan*.[44]

CISA officials told us that CISA has not updated its 2015 *Communications Sector-Specific Plan* because the majority of the plan is still valid; however, these officials also acknowledged that certain elements of the plan are out of date and agreed the plan should be revised. For example, CISA has identified new and emerging threats and risks since 2015 for the Communications Sector. Such threats and risks include information and communications technology supply chain security, and disruptions to position, navigation, and timing services. Further, the plan does not address the National Defense Authorization Act for Fiscal Year 2021 which identifies a number of responsibilities for sector risk management agencies, including CISA.[45] These sector risk management agency responsibilities include supporting critical infrastructure owners and operators by identifying threats; assessing sector risks; sharing information; and supporting incident management and restoration efforts during or following an incident, such as a hurricane, among other responsibilities. An updated plan could also incorporate the results from CISA's assessment of the effectiveness of its programs and services to support the security and resilience of the Communications Sector.

CISA officials stated that DHS plans to publish an updated National Plan by December 31, 2021, but there are no current plans, including any specific dates or time frames, to update the 2015 *Communications*

[43]Department of Homeland Security, *Communications Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan 2013.*

[44]The Communications Sector Coordinating Council and the Communications Sector Government Coordinating Council jointly developed the goals, objectives, and activities in the 2015 *Communications Sector-Specific Plan* with DHS.

[45]Pub. L. No. 116-283, § 9002(c).

Sector-Specific Plan. While publishing an updated National Plan likely will help guide development of an updated sector-specific plan, the current plan is 6 years old, and it may take additional time to apply information from the 2021 National Plan. Developing and issuing a revised *Communications Sector-Specific Plan*, in coordination with public and private Communications Sector stakeholders, would help CISA set goals, objectives, and priorities that address new and emerging threats and risks to the Communications Sector and that are in alignment with its sector risk management agency responsibilities.

Conclusions

CISA has a leadership role in coordinating federal efforts and supporting private sector owners and operators to secure and improve the resilience of the Communications Sector in the face of serious physical, cyber, and human threats. It fulfills its responsibilities through a variety of programs and services to private sector owners and operators. Those programs and services include assessments to improve the physical security of facilities, and information-sharing programs to help detect and respond to cyber threats. Assessing the effectiveness of its programs and services for the Communications Sector will enable CISA to prioritize those efforts that are most useful or relevant to securing and strengthening the resilience of critical infrastructure in the sector and the extent to which these activities are reducing risks.

Also, while CISA is the lead federal agency responsible for coordinating restoration efforts of the Communications Sector through Emergency Support Function #2 after an incident, it has not completed a capability assessment to analyze the resources available to support Emergency Response Function #2 activities. Completing a capability assessment would allow CISA to determine how well Emergency Support Function #2 resources and capabilities align with requirements to support response and restoration efforts during future incidents, such hurricanes and wildfires.

As threats and risks to the Communications Sector continuously evolve, having a plan that reflects CISA's current goals and priorities will help guide CISA's efforts to address new and emerging threats. However, CISA has not updated the 2015 *Communications Sector-Specific Plan* to reflect new emerging threats and risks and its statutory sector risk management agency roles and responsibilities. Further, an updated plan could also incorporate the results from CISA's assessment of the effectiveness of its programs and services to support the sector. Developing and issuing a revised *Communications Sector-Specific Plan*, in coordination with public and private Communications Sector

stakeholders, would help CISA set goals, objectives, and priorities that address new and emerging threats and risks to the Communications Sector and that are in alignment with its sector risk management agency responsibilities.

Recommendations for Executive Action

We are making three recommendations to CISA:

The Director of CISA should assess the effectiveness of CISA's programs and services to support the Communications Sector, including developing and implementing metrics and analyzing feedback received from owners and operators, to determine the usefulness and relevance of its activities to support sector security and resilience. (Recommendation 1)

The Director of CISA should complete a capability assessment for Emergency Support Function #2, such as establishing requirements, maintaining a list of current capabilities, and conducting a capability gap analysis to identify if and where other resources may be needed. (Recommendation 2)

The Director of CISA, in coordination with public and private Communications Sector stakeholders, should produce a revised Communications Sector-Specific Plan, to include goals, objectives, and priorities that address new and emerging threats and risks to the Communications Sector and that are in alignment with sector risk management agency responsibilities. (Recommendation 3)

Agency Comments

We provided a draft of this report to DHS, the Department of Commerce, and the Federal Communications Commission for review and comment. DHS provided written comments, which are reproduced in appendix I. In its comments, DHS concurred with our recommendations and described actions under way or planned to address them. The Department of Commerce and the Federal Communications Commission did not provide comments on the draft report.

With regard to our first recommendation, that CISA assess the effectiveness of its programs and services to support the Communications Sector, DHS concurred and stated that CISA is in the process of refreshing the existing National Infrastructure Protection Plan, which will include metrics to evaluate the activities supporting sector security and resilience. According to DHS, the refreshed National Infrastructure Protection Plan will define CISA's processes and timelines to capture, monitor, assess, measure, and document their overall performance as the sector risk management agency for the

Communications Sector, including through metrics to evaluate the usefulness and relevance of the agency's activities to support sector security and resilience. Further, DHS stated that CISA will incorporate Communications Sector performance metrics and data collection and reporting processes and timelines, including approaches for collecting sector stakeholder feedback in an updated Communications Sector-Specific Plan. DHS estimated that it will complete these efforts by September 30, 2022. At that time, we will assess CISA's actions to determine the extent to which they address the intent of our recommendation.

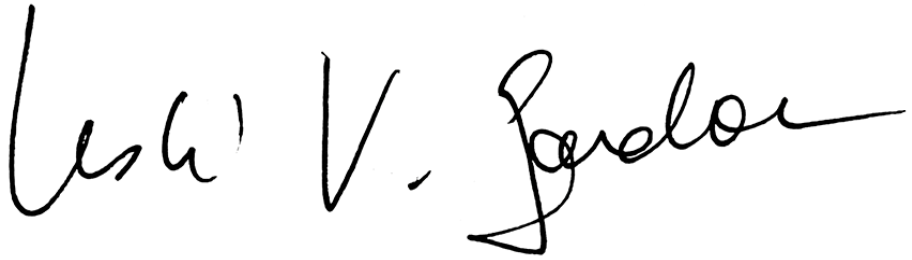
With regard to our second recommendation, that CISA complete a capability assessment for Emergency Support Function #2, DHS concurred and stated that CISA is taking steps to address this recommendation by working with FEMA to update the Communications Annex of both the National Response Framework and the Response and Recovery Federal Interagency Operations Plan. Specifically, DHS stated that updates to these plans will include, among other things, information on the processes and mechanisms for establishing requirements for Emergency Support Function #2. Further, DHS stated that CISA will update and expand the list of Emergency Support Function #2 capabilities and conduct a capability gap analysis to identify where other resources many be needed to support and implement these requirements. DHS estimated that it will complete these efforts by June 30, 2022. At that time, we will assess CISA's actions to determine the extent to which they address the intent of our recommendation.

With regard to our third recommendation, that CISA, in coordination with public and private Communications Sector stakeholders, produce a revised Communications Sector-Specific Plan, DHS concurred and stated that CISA plans to do so upon completion of updates to the National Infrastructure Protection Plan. Specifically, DHS stated that CISA's updated Communications Sector-Specific Plan will, among other things, describe agreed-upon processes and mechanisms by which sector partners identify, prioritize, and address new and emerging threats, as well as goals, objectives, and priorities relating to specific threats within the sector. DHS estimated that it will complete these efforts by September 30, 2022. At that time, we will review the plan to determine if it meets the intent of our recommendation.

We are sending copies of this report to the appropriate congressional committees, the Secretaries of Homeland Security and Commerce, the Chairwoman of the Federal Communications Commission, and other

interested parties. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you or your staffs have any questions about this report, please contact Leslie V. Gordon at 202-512-8777 or GordonLV@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff that made key contributions to this report are listed in appendix II.



Leslie V. Gordon
Acting Director
Homeland Security and Justice Issues

Appendix I: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

November 1, 2021

Leslie V. Gordon
Acting Director, Homeland Security and Justice Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Management Response to Draft Report GAO-22-104462, "CRITICAL INFRASTRUCTURE PROTECTION: CISA Should Assess the Effectiveness of Its Actions to Support the Communications Sector"

Dear Ms. Gordon:

Thank you for the opportunity to comment on this draft report. The U.S. Department of Homeland Security (DHS or the Department) appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing this report.

The Department is pleased to note GAO's recognition that the Cybersecurity and Infrastructure Security Agency (CISA) identifies, categorizes, and characterizes threats to communications networks as a basis to develop and evaluate mitigation measures intended to address threats across the Communications Sector. These efforts are a foundational element of CISA's role as the Sector Risk Management Agency (SRMA) for the Communications Sector, as defined in DHS's 2013 National Infrastructure Protection Plan (National Plan) and clarified in Section 9002 of the January 2021 National Defense Authorization Act (NDAA).

In addition, GAO acknowledged CISA's on-going efforts to support security and resilience in the Communications Sector through information sharing initiatives, incident management and coordination efforts, and a wide range of programs, products, and services offered to Communications Sector partners. CISA remains committed to fulfilling its roles and responsibilities as the SRMA for the Communications Sector and to working with partners across the sector to sustain and strengthen collaborative security and resilience efforts.

The draft report contained three recommendations, with which the Department concurs. Please find attached our detailed response to each recommendation. DHS previously submitted technical comments under a separate cover for GAO's consideration.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Sincerely,

JIM H CRUMPACKER

Digitally signed by JIM H CRUMPACKER
Date: 2021.11.01 15:46:08 -04'00'

JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Attachment

2

Attachment: Management Response to Recommendations Contained in GAO-22-104462

GAO recommended that the CISA Director:

Recommendation 1: Assess the effectiveness of CISA's programs and services to support the Communications Sector, including developing and implementing metrics and analyzing feedback received from owners and operators, to determine the usefulness and relevance of its activities to support sector security and resilience.

Response: Concur. CISA's Infrastructure Security Division (ISD), supported by the Stakeholder Engagement Division (SED), is in the process of refreshing the existing National Plan in response to seminal changes in law, policy, and the risk environment in which the Nation's critical infrastructure operates. This includes the codification and clarification of roles and responsibilities of SRMAs in the January 2021 NDAA which specifies that SRMAs establish and carry out "programs to assist critical infrastructure owners and operators…in identifying, understanding, and mitigating threats, vulnerabilities, and risks to their systems or assets." The NDAA further specifies a government-wide requirement to evaluate and report on the effectiveness of SRMAs in carrying out these responsibilities. Accordingly, the updated National Plan will define processes and timelines by which all SRMAs will capture, monitor, assess, measure, and document their overall performance, including through metrics that evaluate the usefulness and relevance of the activities supporting sector security and resilience.

As the SRMA for the Communications Sector, CISA will also support the Communications Sector in meeting goals articulated in the updated National Plan, such as evaluating and reporting on CISA's effectiveness in carrying out its SRMA responsibilities. For example, CISA SED will incorporate Communications Sector performance metrics and data collection and reporting processes and timelines, including approaches for collecting sector stakeholder feedback, in an updated Communications Sector-Specific Plan. Estimated Completion Date (ECD): September 30, 2022.

Recommendation 2: Complete a capability assessment for Emergency Support Function [ESF] #2, such as establishing requirements, maintaining a list of current capabilities, and conducting a capability gap analysis to identify if and where other resources may be needed.

Response: Concur. CISA's Integrated Operations Division (IOD) is currently engaged in two efforts with FEMA's Recovery Directorate to address this recommendation by updating the: (1) ESF #2 – Communications Annex of the National Response Framework (NRF) dated October 28, 2019; and (2) August 2016 Response and Recovery Federal Interagency Operations Plan, Annex K – Communications. More specifically,

3

CISA IOD updated the terminology, and added Federal Communications Commission core capabilities, to the NRF Communications Annex in September 2021. Further, IOD will: (1) work with FEMA to update Annex K with information on the processes and mechanisms for establishing requirements; (2) further update and expand the list ESF #2 capabilities; and (3) conduct a capability gap analysis to identify where other resources may be needed to support and implement ESF #2 requirements. ECD: June 30, 2022.

Recommendation 3: In coordination with public and private Communications Sector stakeholders, produce a revised Communications Sector-Specific Plan, to include goals, objectives, and priorities that address new and emerging threats and risks to the Communications Sector and that are in alignment with sector risk management agency responsibilities.

Response: Concur. CISA SED will update the Communications Sector-Specific Plan upon completion of updates to the National Plan, which will incorporate key provisions of the January 2021 NDAA that codified and clarified SRMA roles and responsibilities. CISA's update of the Communications Sector-Specific Plan will reflect these updates and incorporate concepts and ideas from completed or ongoing products and initiatives undertaken since the previous Communications Sector-Specific Plan was developed, such as a July 2021 Communications Sector Fact Sheet and a Communications Sector Profile that will be completed by December 2021. Further, the revised Communications Sector-Specific Plan will describe agreed-upon processes and mechanisms by which sector partners identify, prioritize, and address new and emerging threats within the Sector, as well as goals, objectives, and priorities relating to specific threats within the sector. ECD: September 30, 2022.

4

Appendix II: GAO Contact and Staff Acknowledgments

GAO Contact

Leslie V. Gordon at 202-512-8777 or GordonLV@gao.gov

Staff Acknowledgments

In addition to the contact named above, Hugh Paquette (Assistant Director), Jason Jackson (Analyst-in-Charge), Nasreen Badat, Bradley Becker, Benjamin Crossley, Michele Fejfar, Michael Gilmore, David Hinchman, David Hooper, Kenneth Johnson, Carl Potenzieri, and Adam Vogt also contributed to this report. Also contributing to the report were Thomas Baril, Sally Moino, Madhav Panwar, and Sarah Veale.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548

Please Print on Recycled Paper.