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.