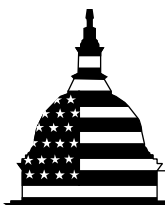


April 2013

COMMUNICATIONS NETWORKS

Outcome-Based Measures Would Assist DHS in Assessing Effectiveness of Cybersecurity Efforts



G A O

Accountability * Integrity * Reliability

Why GAO Did This Study

Ensuring the effectiveness and reliability of communications networks is essential to national security, the economy, and public health and safety. The communications networks (including core and access networks) can be threatened by both natural and human-caused events, including increasingly sophisticated and prevalent cyber-based threats. GAO has identified the protection of systems supporting the nation's critical infrastructure—which includes the communications sector—as a government-wide high-risk area.

GAO was asked to (1) identify the roles of and actions taken by key federal entities to help protect communications networks from cyber-based threats, (2) assess what is known about the extent to which cyber incidents affecting the communications networks have been reported to the FCC and DHS, and (3) determine if Defense's pilot programs to promote cybersecurity in the defense industrial base can be used in the communications sector. To do this, GAO focused on core and access networks that support communication services, as well as critical components supporting the Internet. GAO analyzed federal agency policies, plans, and other documents; interviewed officials; and reviewed relevant reports.

What GAO Recommends

GAO recommends that DHS collaborate with its partners to develop outcome-oriented measures for the communications sector. DHS concurred with GAO's recommendation.

View [GAO-13-275](#). For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov

COMMUNICATIONS NETWORKS

Outcome-Based Measures Would Assist DHS in Assessing Effectiveness of Cybersecurity Efforts

What GAO Found

While the primary responsibility for protecting the nation's communications networks belongs to private-sector owners and operators, federal agencies also play a role in support of their security, as well as that of critical components supporting the Internet. Specifically, private-sector entities are responsible for the operational security of the networks they own, but the Federal Communications Commission (FCC) and the Departments of Homeland Security (DHS), Defense, and Commerce have regulatory and support roles, as established in federal law and policy, and have taken a variety of related actions. For example, FCC has developed and maintained a system for reporting network outage information; DHS has multiple components focused on assessing risk and sharing threat information; Defense and DHS serve as co-chairs for a committee on national security and emergency preparedness for telecommunications functions; and Commerce has studied cyber risks facing the communications infrastructure and participates in standards development. However, DHS and its partners have not yet initiated the process for developing outcome-based performance measures related to the cyber protection of key parts of the communications infrastructure. Outcome-based metrics related to communications networks and critical components supporting the Internet would provide federal decision makers with additional insight into the effectiveness of sector protection efforts.

No cyber-related incidents affecting core and access networks have been recently reported to FCC and DHS through established mechanisms. Specifically, both FCC and DHS have established reporting mechanisms to share information on outages and incidents, but of the outages reported to FCC between January 2010 and October 2012, none were related to common cyber threats. Officials within FCC and the private sector stated that communication networks are less likely to be targeted themselves because they provide the access and the means by which attacks on consumer, business, and government systems can be facilitated.

Attributes of two pilot programs established by Defense to enhance the cybersecurity of firms in the defense industrial base (the industry associated with the production of defense capabilities) could be applied to the communications sector. (See table below.) The department's pilot programs involve partnering with firms to share information about cyber threats and responding accordingly. Considering these attributes can inform DHS as it develops procedures for expanding these pilot programs to all critical infrastructure sectors, including the communications sector.

Relevant Attributes of the Defense Industrial Base Cyber Pilots

| |
|--|
| Agreements |
| Government sharing of unclassified and classified cyber threat information |
| Feedback mechanism on government services |
| Government cyber analysis, mitigation, and digital forensic support |
| Government reporting of voluntarily reported incidents |
| Internet service providers deploying countermeasures based on classified threat indicators for organizations |

Source: GAO analysis of Defense and DHS data.

Contents

| | | |
|--------------|--|----|
| Letter | | 1 |
| | Background | 3 |
| | Agencies Have Taken Action to Address Security of Communications Networks | 12 |
| | Though Reporting Mechanisms Are in Place, FCC and DHS Have Not Received Reports of Cyber-Related Incidents Affecting the Nation's Core and Access Networks | 26 |
| | Attributes of Defense Industry Cybersecurity Pilot Programs Could Be Applied to the Communications Sector | 28 |
| | Conclusions | 31 |
| | Recommendation for Executive Action | 31 |
| | Agency Comments and Our Evaluation | 32 |
| Appendix I | Objectives, Scope, and Methodology | 35 |
| Appendix II | Comments from the Department of Homeland Security | 38 |
| Appendix III | GAO Contact and Staff Acknowledgments | 40 |
| Tables | | |
| | Table 1: Sources of Cybersecurity Threats | 9 |
| | Table 2: Types of Exploits | 11 |
| | Table 3: Federal Communications Commission and Communications Security, Reliability, and Interoperability Council's Key Efforts | 14 |
| | Table 4: Department of Homeland Security Key Efforts | 19 |
| | Table 5: Department of Defense Key Efforts | 22 |
| | Table 6: Department of Commerce Key Efforts | 24 |
| | Table 7: Relevant Attributes of the Defense Industrial Base Cyber Pilots | 29 |
| Figures | | |
| | Figure 1: Communications Networks | 5 |
| | Figure 2: Example Path of Communications | 6 |

| | |
|---|---|
| Figure 3: How the Domain Name System Translates a Website Name into a Numerical Address | 8 |
| Figure 4: Example of Dynamic Routing Using Border Gateway Protocol | 9 |

Abbreviations

| | |
|---------|--|
| CSRIC | Communications Security, Reliability, and Interoperability Council |
| BGP | Border Gateway Protocol |
| CIO | chief information officer |
| DECS | Defense Industrial Base Enhanced Cybersecurity Service |
| DHS | Department of Homeland Security |
| DNS | Domain Name System |
| DNSSEC | Doman Name System Security Extensions |
| DOD | Department of Defense |
| FCC | Federal Communications Commission |
| ICANN | Internet Corporation for Assigned Names and Numbers |
| NIST | National Institute of Standards and Technology |
| NS/EP | national security and emergency preparedness |
| NTIA | National Telecommunications and Information Administration |
| US-CERT | United States Computer Emergency Readiness Team |

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.



United States Government Accountability Office
Washington, DC 20548

April 3, 2013

Congressional Requesters

Effective, reliable communications are essential to our nation's security, economy, and public health and safety. Communications networks have grown increasingly important to American business and consumers, and provide the medium for hundreds of billions of dollars of commerce each year. Further, applications and services (such as telephone calls, e-mail, text messages, chat, file transfers, and video) depend on effectively operating communications networks. The 9/11 terrorist attacks and Hurricanes Katrina and Sandy, in 2005 and 2012, respectively, significantly disrupted communications capabilities and underscore the risks to our nation's complex communications infrastructure. Additionally, such events highlight the need to ensure the availability of communications capabilities for leaders responsible for functions critical to the management of and response to national security and emergency situations. Since 2003, we have identified protecting systems supporting our nation's critical infrastructure (which includes the communications networks)—referred to as cyber-critical infrastructure protection, or cyber CIP—as a government-wide high-risk area, and we continue to do so in the most recent update to our high-risk list.¹

In light of the importance of the security of the nation's communications infrastructure, you asked us to (1) identify the roles of and actions taken by key federal entities to help protect the communications networks from cyber-based threats, (2) assess what is known about the extent to which cyber-incidents affecting the communications networks have been reported to the Federal Communications Commission (FCC) and the Department of Homeland Security (DHS), and (3) determine if the Department of Defense's (DOD) pilot programs to promote cybersecurity in the defense industrial base can be used in the communications sector. To identify the roles and actions taken by key federal agencies, we

¹GAO's biennial high-risk list identifies government programs that have greater vulnerability to fraud, waste, abuse, and mismanagement or need transformation to address economy, efficiency, or effectiveness challenges. We have designated federal information security as a high-risk area since 1997; in 2003, we expanded this high-risk area to include protecting systems supporting our nation's critical infrastructure. See, most recently, GAO, *High-Risk Series: An Update*, [GAO-13-283](#) (Washington, D.C.: February 2013).

focused on two of the main functional components of the communications networks that facilitate communications services for the nation as well as critical components supporting the Internet.² Further, we focused on agencies with primary responsibility for supporting the cybersecurity of the communications networks: FCC and the Departments of Commerce, Homeland Security, and Defense. For each agency, we analyzed policy, strategic plans, guidance, and related performance metrics and interviewed officials. Additionally, we reviewed documents from and conducted interviews with officials from the Communications Information Sharing and Analysis Center to assess federal efforts to fulfill roles and responsibilities.³

To assess what is known about the extent to which cyber-incidents affecting the communications networks have been reported to the federal government, we reviewed evidence regarding incidents in the communications sector reported through established mechanisms at FCC and DHS from January 2010 to October 2012. This enabled us to identify any cyber-related incidents related to the two main functional components of the communications networks. We also reviewed publicly published reports by information security firms and communications network companies to determine if communications network-related cyber incidents were reported.

To determine if DOD's pilot can be used to inform the communications sector, we reviewed our August 2012 report on DOD efforts to enhance the cybersecurity of the defense industrial base critical infrastructure sector.⁴ We then identified and summarized attributes of the program that

²We focused on core and access networks. Core networks transport a high volume of aggregated traffic over substantial distances or between different service providers or "carriers." Access networks are primarily local portions of the 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 and various Internet-based services. We did not focus on services provided directly to the end users or customers, sometimes referred to as the "last mile" by the industry.

³Information-sharing and analysis centers were established to serve an operational role such as providing mechanisms for gathering, analyzing, and disseminating information on physical and cyber-related infrastructure threats and vulnerabilities to and from private infrastructure sectors and the government.

⁴GAO, *Defense Cyber Efforts: Management Improvements Needed to Enhance Programs Protecting the Defense Industrial Base from Cyber Threats*, GAO-12-762SU (Washington, D.C.: Aug. 3, 2012). This report is restricted to official use only and is not publicly available.

could be publicly reported and that were potentially applicable to the communications sector.

We conducted this performance audit from April 2012 to April 2013 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. Appendix I contains additional details on the objectives, scope, and methodology of our review.

Background

The national information and communications networks consist of a collection of mostly privately owned networks that are critical to the nation's security, economy, and public safety. The communications sector operates these networks and is comprised of public- and private-sector entities that have a role in, among other things, the use, protection, or regulation of the communications networks and associated services (including Internet routing).⁵ For example, private companies, such as AT&T and Verizon, function as service providers, offering a variety of services to individual and enterprise end users or customers.

The modern communications network is a network of networks and includes the basis for the operation of the Internet.⁶ The nation's communications networks include multiple components: core networks, access networks, and end-user technology (e.g., wired phones, cell phones, and computers). The core and access networks facilitate communication so that services (e.g., voice and data) can be provided to

⁵Communications is one of 18 critical infrastructure sectors established by federal policy. The other sectors are agriculture and food; banking and finance; chemical; commercial facilities; critical manufacturing; dams; defense industrial base; emergency services; energy; government facilities; health care and public health; information technology; national monuments and icons; nuclear reactors, materials, and waste; postal and shipping; transportation systems; and water.

⁶The Internet is a vast network of interconnected networks. It is used by governments, businesses, research institutions, and individuals around the world to communicate, engage in commerce, do research, educate, and entertain.

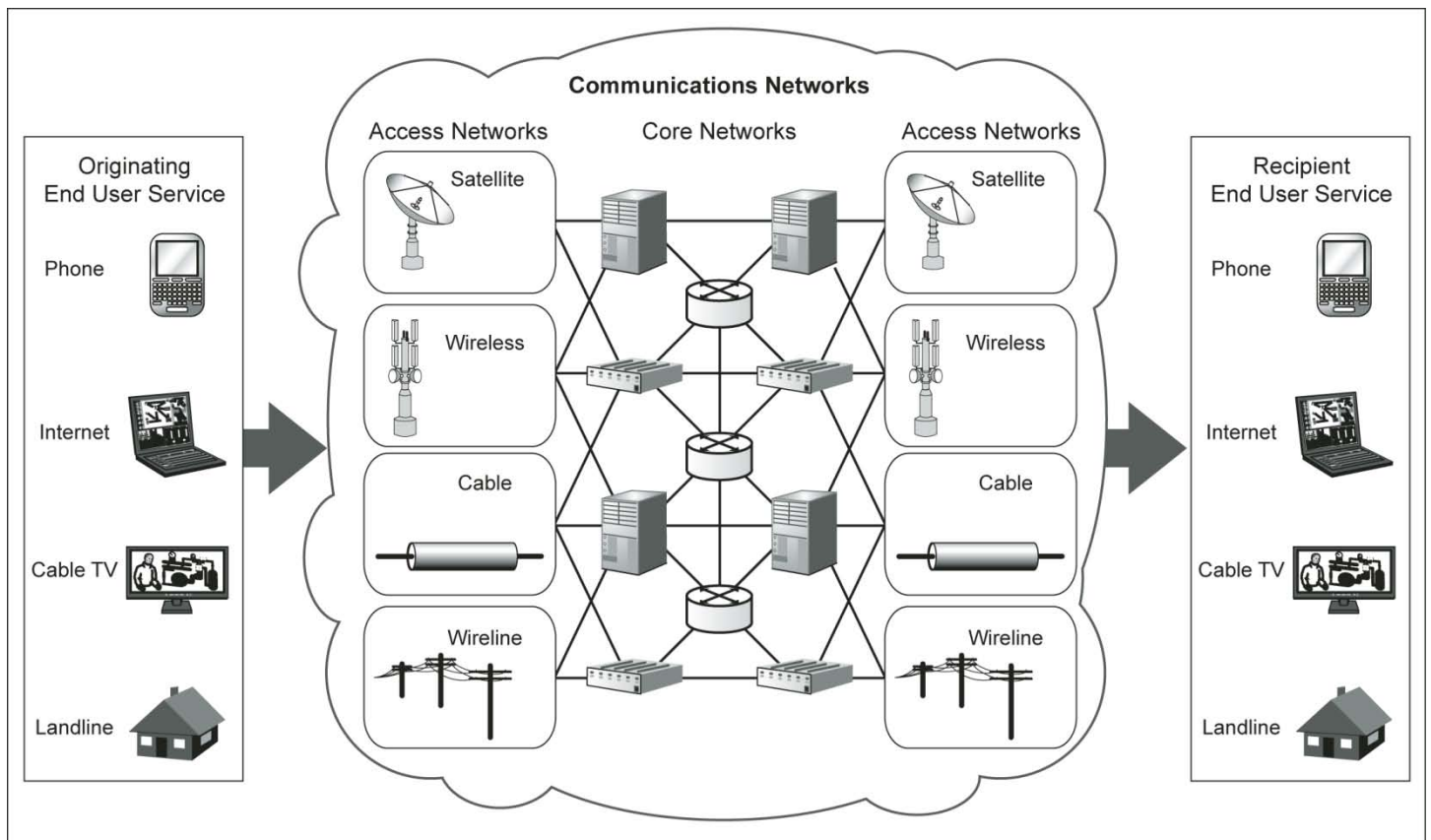
customers that are positioned at the ends of the network, or the “last mile,” as referred to by industry.⁷

- The core networks transport a high volume of aggregated traffic⁸ over substantial distances or between different service providers or “carriers.” 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 to transmit data, service providers manage and control core infrastructure elements with numerous components, including signaling systems, databases, switches, routers, and operations centers. Multiple service providers, such as AT&T and Verizon, operate distinct core networks traversing the nation that interconnect with each other at several points. End users generally do not connect directly with the core networks.
- Access networks are primarily local portions of the 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, including fixed and portable systems; wireless, including cellular base stations; cable, including video, data, and voice systems, and cable system end offices; and wireline, including voice and data systems and end offices. Communications traffic between two locations may originate and terminate within an access network without connecting to core networks (e.g., local phone calling within the wireline network). Communications traffic between different types of access networks (e.g., between the wireline and wireless networks) may use core networks to facilitate the transmission of traffic. Individual and enterprise users connect to access networks through various devices (e.g., wired phones, cell phones, and computers). Figure 1 depicts the interconnection of user devices and services, access networks, and core networks. Figure 2 depicts the path that a single communication can take to its final destination.

⁷The “last mile” refers to communications technology that bridge the transmission distance between the service provider and the customer.

⁸Aggregate traffic is normally the multimedia (voice, data, video) traffic combined from different service providers, or carriers, to be transported over high-speed through the core networks.

Figure 1: Communications Networks

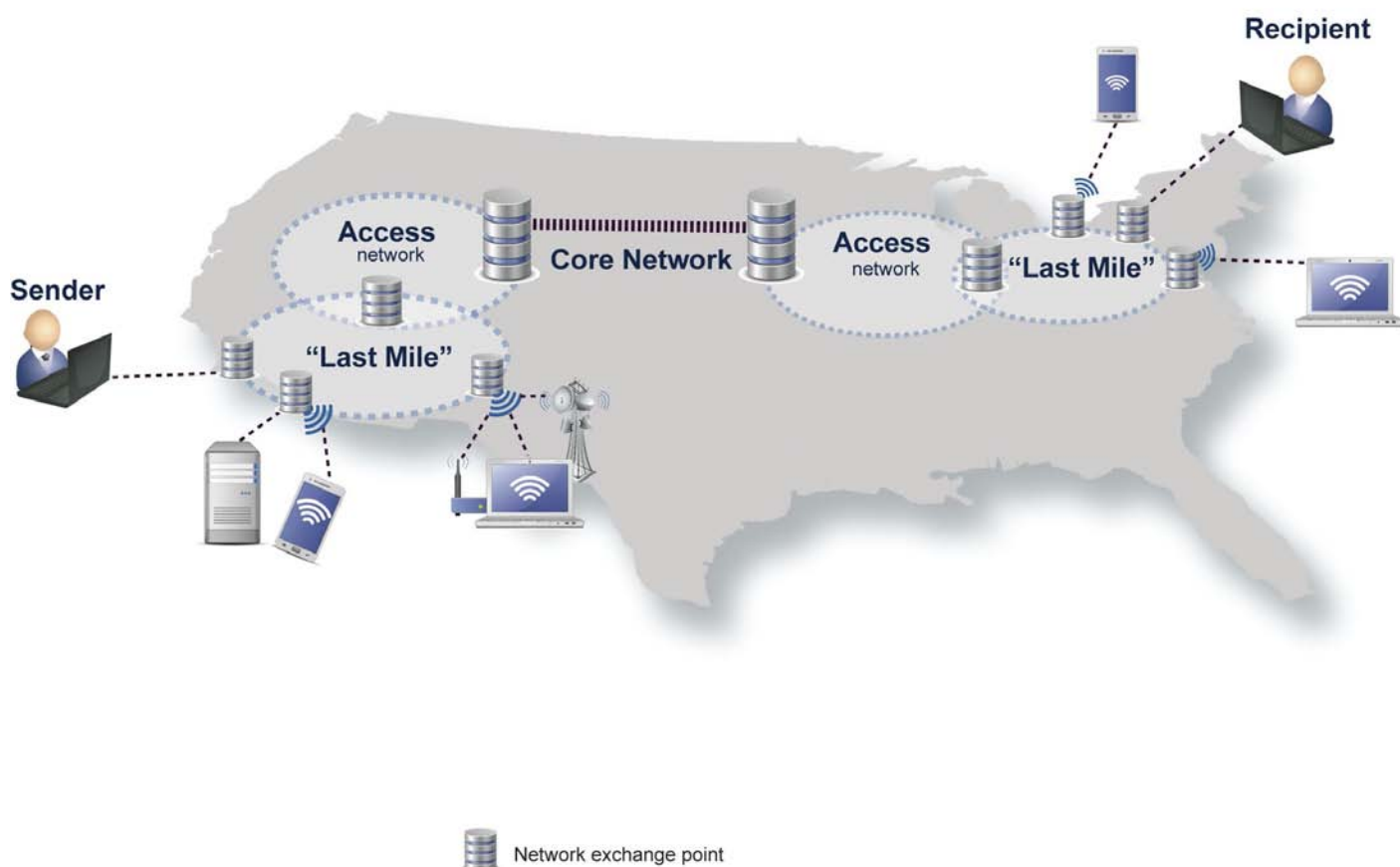


Source: GAO analysis of communications sector data.

Figure 2: Example Path of Communications

Interactive graphic

Directions:  Roll over each  below to view more information.



Source: GAO analysis of communications sector data.

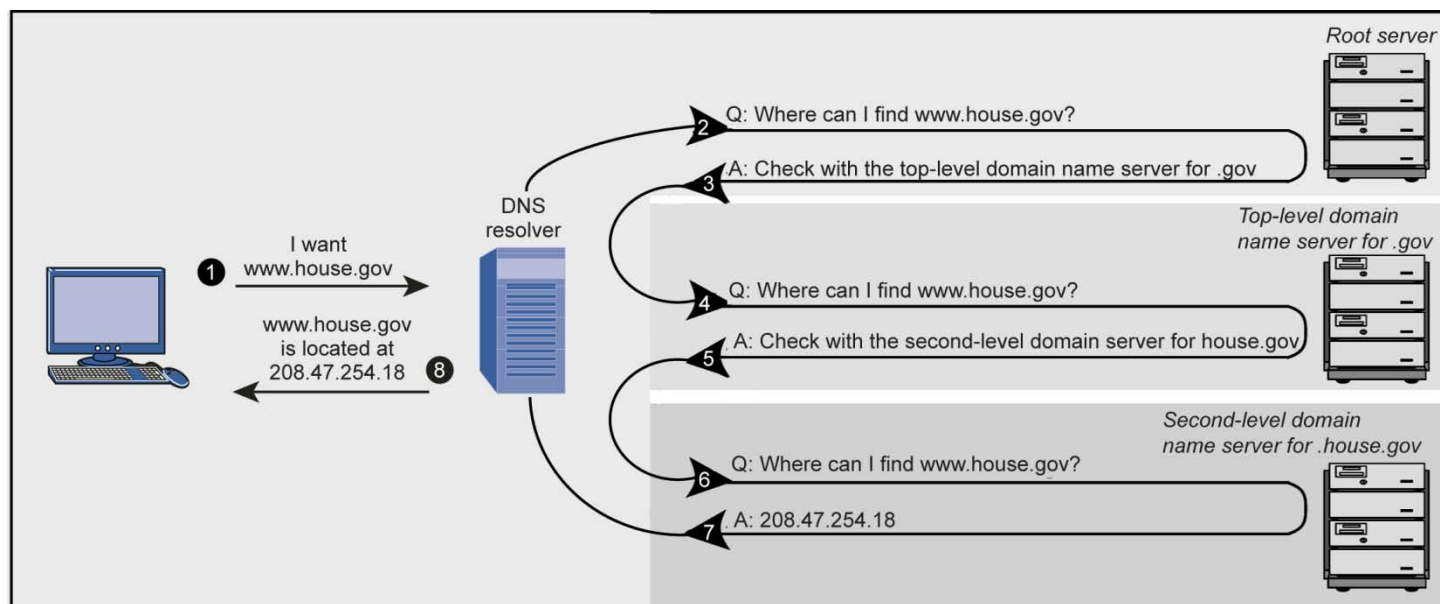
Critical Protocols Supporting the Internet

The nation's communications infrastructure also provides the networks that support the Internet. In order for data to move freely across communications networks, the Internet network operators employ voluntary, self-enforcing rules called protocols. Two sets of protocols—the Domain Name System (DNS) and the Border Gateway Protocol (BGP)—are essential for ensuring the uniqueness of each e-mail and website address and for facilitating the routing of data packets between autonomous systems, respectively.⁹

DNS provides a globally distributed hierarchical database for mapping unique names to network addresses. It links e-mail and website addresses with the underlying numerical addresses that computers use to communicate with each other. It translates names, such as <http://www.house.gov>, into numerical addresses, such as 208.47.254.18, that computers and other devices use to identify each other on the network and back again in a process invisible to the end user. This process relies on a hierarchical system of servers, called domain name servers, which store data linking address names with address numbers. These servers are owned and operated by many public and private sector organizations throughout the world. Each of these servers stores a limited set of names and numbers. They are linked by a series of root servers that coordinate the data and allow users' computers to find the server that identifies the sites they want to reach. Domain name servers are organized into a hierarchy that parallels the organization of the domain names (such as ".gov", ".com", and ".org"). Figure 3 below provides an example of how a DNS query is turned into a number.

⁹Autonomous systems are the mechanism to aggregate large groups of computers (e.g., Internet protocol addresses) into single networks—such as that of a specific Internet service provider or organization.

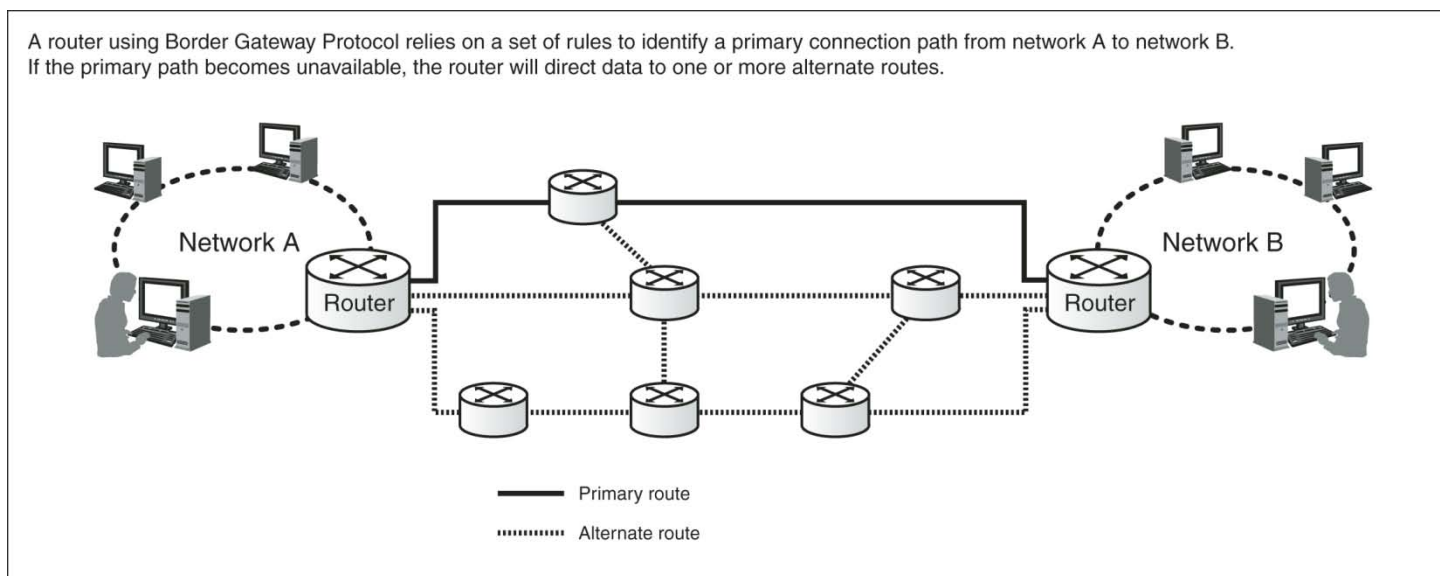
Figure 3: How the Domain Name System Translates a Website Name into a Numerical Address



Source: GAO analysis of a prior GAO report and DHS data.

BGP is used by routers located at network nodes to direct traffic across the Internet. Typically, routers that use this protocol maintain a routing table that lists all feasible paths to a particular network. They also determine metrics associated with each path (such as cost, stability, and speed) and follow a set of constraints (e.g., business relationships) to choose the best available path for forwarding data. This protocol is important because it binds together many autonomous networks that comprise the Internet (see fig. 4).

Figure 4: Example of Dynamic Routing Using Border Gateway Protocol



Source: GAO analysis of a prior GAO report.

Threats to the Communications Networks

Like those affecting other cyber-reliant critical infrastructure, threats to the communications infrastructure can come from a wide array of sources. These sources include corrupt employees, criminal groups, hackers, and foreign nations engaged in espionage and information warfare. These threat sources vary in terms of the capabilities of the actors, their willingness to act, and their motives, which can include monetary gain or political advantage, among others. Table 1 describes the sources in more detail.

Table 1: Sources of Cybersecurity Threats

| Threat source | Description |
|-----------------------|---|
| Bot-network operators | Bot-net operators use a network, or bot-net, of compromised, remotely controlled systems to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. The services of these networks are sometimes made available on underground markets (e.g., purchasing a denial-of-service attack or services to relay spam or phishing attacks). |
| Criminal groups | Criminal groups seek to attack systems for monetary gain. Specifically, organized criminal groups use spam, phishing, and spyware/malware to commit identity theft, online fraud, and computer extortion. |

| Threat source | Description |
|-------------------------------|--|
| Hackers | Hackers break into networks for the thrill of the challenge, bragging rights in the hacker community, revenge, stalking, monetary gain, and political activism, among other reasons. While gaining unauthorized access once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use. According to the Central Intelligence Agency, the large majority of hackers do not have the requisite expertise to threaten difficult targets such as critical U.S. networks. Nevertheless, the worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage. |
| Insiders | The disgruntled or corrupt organization insider is a source of computer crime. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat includes contractors hired by the organization, as well as careless or poorly trained employees who may inadvertently introduce malware into systems. |
| International corporate spies | International corporate spies pose a threat to the United States through their ability to conduct economic and industrial espionage ^a and large-scale monetary theft and to hire or develop hacker talent. |
| Nations | Nations use cyber tools as part of their information-gathering and espionage activities, including economic espionage directed against U.S. businesses. In addition, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. In his January 2012 testimony, the Director of National Intelligence stated that, among state actors, China and Russia are of particular concern. |
| Phishers | Individuals or small groups execute phishing schemes in an attempt to steal identities or information for monetary gain. Phishers may also use spam and spyware or malware to accomplish their objectives. |
| Spammers | Individuals or organizations distribute unsolicited e-mail with hidden or false information in order to sell products, conduct phishing schemes, distribute spyware or malware, or attack organizations (e.g., a denial of service). |
| Spyware or malware authors | Individuals or organizations with malicious intent carry out attacks against users by producing and distributing spyware and malware. Several notable destructive computer viruses and worms have harmed files and hard drives, and caused physical damage to equipment, including the Melissa Macro Virus, the Explore.Zip worm, the CIH (Chernobyl) Virus, Nimda, Code Red, Slammer, Blaster, and Stuxnet. |
| Terrorists | Terrorists seek to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the economy, and damage public morale and confidence. Terrorists may use phishing schemes or spyware/malware in order to generate funds or gather sensitive information. |

Source: GAO analysis based on data from the Director of National Intelligence, Department of Justice, Central Intelligence Agency, National Institute of Standards and Technology, and the Software Engineering Institute's CERT® Coordination Center.

^aAccording to the Office of the National Counterintelligence Executive, industrial espionage, or theft of trade secrets, occurs when an actor, intending or knowing that his or her offense will injure the owner of a trade secret of a product produced for or placed in interstate or foreign commerce, acts with the intent to convert that trade secret to the economic benefit of anyone other than the owner. See *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011* (October 2011).

These sources may make use of various cyber techniques, or exploits, to adversely affect communications networks, such as denial-of-service

attacks, phishing, passive wiretapping, Trojan horses, viruses, worms, and attacks on the information technology supply chains that support the communications networks. Table 2 provides descriptions of these cyber exploits.

Table 2: Types of Exploits

| Type of exploit | Description |
|--|--|
| Denial-of-service | An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources. |
| Distributed denial-of-service | A variant of the denial-of-service attack that uses numerous hosts to perform the attack. |
| Phishing | A digital form of social engineering that uses authentic-looking, but fake, e-mails to request information from users or direct them to a fake website that requests information. |
| Passive wiretapping | The monitoring or recording of data, such as passwords transmitted in clear text, while they are being transmitted over a communications link. This is done without altering or affecting the data. |
| Trojan Horse | A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms by, for example, masquerading as a useful program that a user would likely execute. |
| Virus | A computer program that can copy itself and infect a computer without the permission or knowledge of the user. A virus might corrupt or delete data on a computer, use e-mail programs to spread itself to other computers, or even erase everything on a hard disk. Unlike a computer worm, a virus requires human involvement (usually unwitting) to propagate. |
| Worm | A self-replicating, self-propagating, self-contained program that uses network mechanisms to spread itself. Unlike computer viruses, worms do not require human involvement to propagate. |
| Exploits affecting the information technology supply chain | The installation of hardware or software that contains malicious logic (like logic bombs, Trojan horses, or viruses) or unintentional vulnerabilities (the result of existing defects, such as coding errors) or that may be counterfeited. Supply chain threats can also come from the failure or disruption in the production of critical product, or a reliance on a malicious or unqualified service provider for the performance of technical services. |

Source: GAO analysis of unclassified governmental and nongovernmental data.

In addition to cyber-based threats, the nation's communications networks also face threats from physical sources. Examples of these threats include natural events (e.g., hurricanes or flooding) and man-made disasters (e.g., terrorist attacks), as well as unintentional man-made outages (e.g., a backhoe cutting a communication line).

Agencies Have Taken Action to Address Security of Communications Networks

While the private sector owns and operates the nation's communications networks and is primarily responsible for protecting these assets, federal law and policy establish regulatory and support roles for the federal government in regard to the communications networks. In this regard, federal law and policy call for critical infrastructure protection activities that are intended to enhance the cyber and physical security of both the public and private infrastructures that are essential to national security, national economic security, and public health and safety. The federal role is generally limited to sharing information, providing assistance when asked by private-sector entities, and exercising regulatory authority when applicable.

As part of their efforts in support of the security of communications networks, FCC, DHS, DOD, and Commerce have taken a variety of actions, including ones related to developing cyber policy and standards, securing Internet infrastructure, sharing information, supporting national security and emergency preparedness (NS/EP), and promoting sector protection efforts.¹⁰

Federal Communications Commission

FCC is a U.S. government agency that regulates interstate and international communications by radio, television, wire, satellite, and cable throughout the United States.¹¹ Its regulations include requirements for certain communications providers to report on the reliability and security of communications infrastructures. These include disruption-reporting requirements for outages that are defined as a significant degradation in the ability of an end user to establish and maintain a

¹⁰On February 12, 2013, the President signed Executive Order 13636 and issued Presidential Policy Directive 21 to improve critical infrastructure cybersecurity and advance efforts to strengthen and maintain secure, functioning, and resilient critical infrastructure, respectively. The executive order, which was published in the Federal Register at 78 Fed. Reg. 11739 (Feb. 19, 2013), prescribes actions to be taken by federal agencies, including the Departments of Defense, Homeland Security, and Commerce (including the National Institute of Standards and Technology), related to enhancing cybersecurity. In addition, the directive details responsibilities of federal agencies related to critical infrastructure security and resilience, including those of FCC and the Department of Commerce. While these responsibilities and actions will impact protection efforts across all critical infrastructures, the specific impact on the communications sector is unknown at this time.

¹¹FCC's major statutory authority is the Communications Act of 1934, as amended, including by the Telecommunications Act of 1996, Pub. L. No. 104-104 (Feb. 8, 1996); 47 U.S.C. Ch. 5, et al.

channel of communications as a result of failure or degradation in the performance of a communications provider's network.

The Commission's Public Safety and Homeland Security Bureau has primary responsibility for assisting providers in ensuring the security and availability of the communications networks.¹² The bureau also serves as a clearinghouse for public safety communications information and emergency response issues. In addition, its officials serve as Designated Federal Officers¹³ on the Communications Security, Reliability, and Interoperability Council.

The Communications Security, Reliability, and Interoperability Council is a federal advisory committee whose mission is to provide recommendations to FCC to help ensure, among other things, secure and reliable communications systems, including telecommunications, media, and public safety systems. The council has provided recommendations in the form of voluntary best practices that provide companies with guidance aimed at improving the overall reliability, interoperability, and security of networks. Specifically, it is composed of 11 working groups that consist of experts from industry and other federal agencies. The working groups focus on various related topics, including those related to network security management, as well the security of the Border Gateway Protocol and the Domain Name System. The working groups develop recommendations through industry cooperation and voluntary agreements. For example, in March 2012, the commission announced the voluntary commitments by the nation's largest Internet service providers, including AT&T and Verizon, to adopt the council's recommendations aimed at better securing their communications networks. The recommendations covered a variety of security practices, including those related to the security of the Domain Name System and BGP.

¹²To fulfill the Commission's mission, FCC is organized in various bureaus and offices that are responsible for overseeing different aspects of the nation's communications networks. In addition to the Public Safety and Homeland Security Bureau, others include Consumer and Governmental Affairs, Enforcement, Wireline Competition, Wireless Telecommunications, Engineering and Technology, and Media.

¹³The designated federal officer (DFO) will approve or call all of the advisory committee's and subcommittees' meetings, prepare and approve all meeting agendas, attend all committee and subcommittee meetings, adjourn any meeting when the DFO determines adjournment to be in the public interest, and chair meetings when directed to do so by FCC Chairman.

The key FCC and council efforts related to the security of the communications sector are detailed in table 3 below.

Table 3: Federal Communications Commission and Communications Security, Reliability, and Interoperability Council’s Key Efforts

| Component | Action |
|--|--|
| Public Safety and Homeland Security Bureau | <p>Developed and maintains the Disaster Information Reporting System, a voluntary, web-based system used by members of the communications sector to track the status of the restoration of communications in the event of a large-scale disaster. The system can provide situational awareness information on the status of restoration efforts to government partners in FCC and DHS.</p> <p>Developed and maintains the Network Outage Reporting System.^a Members of the communications sector submit reports through the system that include detailed information about the causes of network outages and the methods used to restore service.</p> <p>Conducts monthly reviews of the Network Outage Reporting System reports to identify any trends in the causes of the outages, which could potentially be reported to industry working groups on a quarterly basis for them to investigate and make related recommendations.</p> <p>Investigates reasons why systemic or recurring outages occur and makes informal, nonbinding recommendations to responsible carriers regarding options for improving reliability.</p> <p>Recommends enforcement actions against carriers that do not fulfill outage reporting requirements.</p> <p>Provides support to facilitate the overall Communications Security, Reliability, and Interoperability Council process and functions as a liaison for the various working groups.</p> |
| Communications Security, Reliability, and Interoperability Council | <p>Issued reports with voluntary recommendations to Internet service providers related to</p> <ul style="list-style-type: none"> evaluating existing BGP security metrics and extending them to providers where necessary;^b establishing a minimal threshold of Domain Name System Security Extensions (DNSSEC) implementation;^c and performing continuous monitoring and analysis of BGP security incidents.^d <p>Issued best practices, through voluntary agreements with industry partners, related to a variety of topics, including cybersecurity and network security.^e</p> |

Source: GAO analysis of FCC data.

^aThe Network Outage Reporting System is a mandatory reporting system for outages that meet a minimum threshold of 900,000 user minutes, which are calculated by multiplying the number of affected users by the length of the outage. Thus, an outage that affected 30,000 users for a minimum of 30 minutes would meet the threshold of 900,000 user minutes.

^bCommunications Security, Reliability and Interoperability Council (CSRIC), *Secure BGP Deployment*, (March 2012).

^cCSRIC, *DNSSEC Implementation Practices for ISPs* (March 2012). DNSSEC provides cryptographic protections to DNS communication exchanges, thereby reducing threats of DNS-based attacks and improving the overall integrity and authenticity of information processed over the Internet.

^dCSRIC, *Secure BGP Deployment*.

^eCSRIC, *Cyber Security Best Practices* (March 2011) and *Network Security Best Practices* (September 2012).

Department of Homeland Security

DHS is the principal federal agency to lead, integrate, and coordinate the implementation of efforts to protect cyber-critical infrastructures. DHS's role in critical infrastructure protection is established by law and policy. The Homeland Security Act of 2002,¹⁴ Homeland Security Presidential Directive 7,¹⁵ and the National Infrastructure Protection Plan¹⁶ establish a cyber protection approach for the nation's critical infrastructure sectors—including communications—that focuses on the development of public-private partnerships and establishment of a risk management framework. These policies establish critical infrastructure sectors, including the communications sector; assign agencies to each sector (sector-specific agencies), including DHS as the sector lead for the communications and information technology sectors; and encourage private sector involvement through the development of sector coordinating councils, such as the Communications Sector Coordinating Council, and information-sharing mechanisms, such as the Communications Information Sharing and Analysis Center.

¹⁴Homeland Security Act of 2002, Pub. L. No. 107-296 (Nov. 25, 2002). The act created the Department of Homeland Security. In addition, among other things, it assigned the department the critical infrastructure protection responsibility of developing a comprehensive national plan for securing the key resources and critical infrastructures of the United States.

¹⁵The White House, Homeland Security Presidential Directive 7 (Washington, D.C.: Dec. 17, 2003). The directive assigned responsibilities for DHS and other federal agencies focused on specific critical infrastructure sectors. These sector-specific agencies are responsible for identifying, prioritizing, and coordinating the protection of critical infrastructure to prevent, deter, and mitigate the effects of attacks. As of February 12, 2013, Presidential Policy Directive 21 revoked Homeland Security Presidential Directive 7. However, the policy directive continues to assign sector-specific agencies and states that plans developed pursuant to Homeland Security Presidential Directive 7 shall remain in effect until specifically revoked or superseded.

¹⁶DHS, *National Infrastructure Protection Plan, Partnering to Enhance Protection and Resiliency* (Washington, D.C.: January 2009). This plan sets forth a risk management framework and details the roles and responsibilities of DHS; sector-specific agencies; and other federal, state, regional, local, tribal, territorial, and private sector partners, including how they should use risk management principles to prioritize protection activities within and across sectors. Presidential Policy Directive 21 directed the Secretary of Homeland Security to update the National Infrastructure Protection Plan by October 2013.

Additionally, DHS has a role, along with agencies such as DOD, in regard to national security and emergency preparedness (NS/EP)¹⁷ communications that are intended to increase the likelihood that essential government and private-sector individuals can complete critical phone calls and organizations can quickly restore service during periods of disruption and congestion resulting from natural or man-made disasters. In particular, Executive Order No.13618 established an NS/EP Communications Executive Committee to serve as an interagency forum to address such communications matters for the nation.¹⁸ Among other things, the committee is to advise and make policy recommendations to the President on enhancing the survivability, resilience, and future architecture for NS/EP communications. The Executive Committee is composed of Assistant Secretary-level or equivalent representatives designated by the heads of the Departments of State, Defense, Justice, Commerce, and Homeland Security, the Office of the Director of National Intelligence, the General Services Administration, and the Federal Communications Commission, as well as such additional agencies as the Executive Committee may designate. The committee is chaired by the DHS Assistant Secretary for the Office of Cybersecurity and Communications and the DOD Chief Information Officer, with administrative support for the committee provided by DHS.

To fulfill DHS's cyber-critical infrastructure protection and NS/EP-related missions, the Office of Cybersecurity and Communications within the National Protection and Programs Directorate¹⁹ is responsible for, among

¹⁷According to Executive Order No. 13618, Assignment of National Security and Emergency Preparedness Communications Functions, 77 Fed. Reg. 40779 (July 11, 2012), NS/EP refers to the federal government's need to have the ability to communicate at all times and under all circumstances to carry out its most critical and time-sensitive missions. Survivable, resilient, enduring, and effective communications, both domestic and international, are essential to enable the executive branch to communicate within itself and with the legislative and judicial branches; state, local, territorial, and tribal governments; private sector entities; and the public, allies, and other nations. Such communications must be possible under all circumstances to ensure national security, effectively manage emergencies, and improve national resilience.

¹⁸Executive Order No. 13618 revoked Executive Order 12472 (Apr. 3, 1984), which gave the National Communications System responsibility for NS/EP telecommunications. The management of NCS was assigned to DHS after DHS's creation in 2002. Those functions were realigned within DHS following the issuance of Executive Order 13618.

¹⁹The National Protection and Programs Directorate is one of the 24 components that comprise DHS.

other things, ensuring the security, resiliency, and reliability of the nation's cyber and communications infrastructure, implementing a cyber-risk management program for protection of critical infrastructure, and planning for and providing national security and emergency preparedness communications to the federal government.

The office is made up of the following five subcomponents that have various responsibilities related to DHS's overarching cybersecurity mission:²⁰

- Stakeholder Engagement and Cyber Infrastructure Resilience division, among other things, is responsible for managing the agency's role as the sector-specific agency for the communications sector.²¹
- Office of Emergency Communications is responsible for leading NS/EP and emergency communications in coordination and cooperation with other DHS organizations.
- National Cybersecurity and Communications Integration Center is the national 24-hours-a-day, 7-days-a-week operations center that is to provide situational awareness, multiagency incident response, and strategic analysis for issues related to cybersecurity and NS/EP communications. The center is comprised of numerous co-located, integrated elements including the National Coordinating Center for Telecommunications,²² the U.S. Computer Emergency Readiness

²⁰Prior to the issuance of Executive Order 13618 in July 2012, the Office of Cybersecurity and Communications was divided into three components: The Office of Emergency Communications, the National Cyber Security Division, and the National Communications System. Based on the requirements of the executive order, DHS realigned the Office of Cybersecurity and Communications into five divisions.

²¹Prior to Executive Order 13618, DHS's NCS division was designated within DHS to serve as the sector-specific agency for the communications sector.

²²The National Coordinating Center is a joint industry-government center involving members of the U.S. telecommunications industry and the federal government that work to assist in the initiation, coordination, restoration, and reconstitution of NS/EP telecommunications services or facilities. The center was established in January 1984 and was originally a component of the National Communications System.

Team (US-CERT),²³ and the Industrial Control Systems Cyber Emergency Response Team.²⁴

- Federal Network Resilience division is responsible for collaborating with departments and agencies across the federal government to strengthen the operational security of the “.gov” networks. As part of those efforts, the division leads the DHS initiative related to DNSSEC.
- Network Security Deployment division is responsible for designing, developing, acquiring, deploying, sustaining, and providing customer support for the National Cybersecurity Protection System.²⁵

Four of these subcomponents have taken specific actions with respect to the communications networks, which are detailed in table 4 below.

²³The U.S. Computer Emergency Readiness Team is tasked with implementing certain DHS cybersecurity responsibilities, including coordinating and collaborating with public, private, and international partners to help protect and defend the nation’s interests against threats from cyberspace.

²⁴The Industrial Control Systems Cyber Emergency Response Team coordinates control systems-related security incidents and information sharing with federal, state, and local agencies and organizations, the intelligence community, and private sector constituents, including vendors, owners and operators, and international and private sector computer security incident response teams.

²⁵The National Cybersecurity Protection System is a program aimed at reducing the federal government’s vulnerability to cyber threats by decreasing the frequency of cyberspace disruptions and minimizing the duration and damage of those disruptions. According to DHS, it is expected to provide capabilities in four cyber mission areas: (1) threat alert, warning, and analysis; (2) coordination and collaboration; (3) response and assistance; and (4) protection and detection.

Table 4: Department of Homeland Security Key Efforts

| Component | Action |
|--|---|
| Stakeholder Engagement and Cyber Infrastructure Resilience | <p>Completed the Communications Sector annual report to identify, prioritize, and coordinate Critical Infrastructure and Key Resources protection progress and requirements.</p> <p>Issued the Communications Sector-specific risk assessment that outlines the specific physical and cyber risks faced by the sector as a whole.</p> <p>Completed, in coordination with the sector representatives, the Communications Sector Specific Plan that describes how the communications sector plans to manage risk utilizing both public and private resources; how partners will implement programs and practices to achieve sector goals, including addressing cybersecurity; and how the sector will measure the success of protective activities.</p> <p>Coordinates and serves as the Executive Secretariat support to the President's National Security Telecommunications Advisory Committee.^a</p> <p>Manages the Network Security Information Exchange, which is an information-sharing working forum related to NS/EP in the communications and information technology sectors. It includes communications sector officials that meet every 2 months to share actionable and relevant threat and vulnerability information in a secure environment. Additionally, the Network Security Information Exchanges holds multilateral exchange meetings with its counterparts from the United Kingdom, Canada, Australia, and New Zealand.</p> <p>Manages the Joint Program Office to support the new Executive Committee for NS/EP Telecommunications required by Executive Order 13618. Actions taken related to the executive committee include creating a charter for the committee (approved in September 2012), developing a staffing and resource plan for the Joint Program Office, planning the specific tasks defined in the executive order, evaluating the current status and integration of existing efforts, and discussing how the dismantling of the National Communications System impacts NS/EP telecommunications functions.</p> |
| Office of Emergency Communications | <p>Operates a variety of analysis tools that provide support of the office's ability to fulfill NS/EP activities. For example, the Infrastructure Mapping Tool provides detailed analysis of the nation's communications infrastructure by providing detailed information (e.g., location and type) about nodes and switches within the communications infrastructure as well as information on the owners of the various components. This can assist with assessment of potential impacts that may occur as a result of all types of disasters (e.g., earthquakes or hurricanes), which are shared with the communications service providers.</p> <p>Issued the National Emergency Communications Plan intended to unify and lead a nationwide effort to improve NS/EP and emergency communications capabilities across all levels of the government.</p> |

| Component | Action |
|--|---|
| National Cybersecurity and Communications Integration Center | <p>Coordinates and collaborates with public, private, and international partners to help protect and defend the nation's interests against threats from cyberspace.</p> <p>Receives, integrates, analyzes, and disseminates communications-related information to federal, state, and local partners as well as the private sector in order to establish communications situational awareness, and priority-setting recommendations.</p> <p>Serves as a joint industry-government operations center with the mission to coordinate response and restoration priorities during an incident.</p> <p>Established mechanisms to share information about threats, vulnerabilities, intrusions, and anomalies through its Communications Information Sharing and Analysis function.</p> <p>Oversees the Cyber Exercise Program, which is an initiative aimed at improving the nation's cybersecurity readiness, protection, and incident response capabilities by conducting various exercises, including Cyberstorm.</p> <p>Leads efforts related to the National Response Framework's Emergency Support Function 2, which support the restoration of the communications infrastructure, facilitate the recovery of systems and applications from cyber attacks, and coordinate federal communications support to response efforts during incidents that require a coordinated federal response.^b</p> |
| Federal Network Resilience | <p>Issued DNS Security Reference Architecture, which is guidance aimed at optimizing and standardizing the DNS currently in use by the federal civilian government and improving the federal government's security posture by reducing the threats against the DNS at federal civilian agencies.</p> |

Source: GAO analysis of DHS data.

^aThe National Security Telecommunications Advisory Committee is a presidential advisory group, comprised of chief executives from major telecommunications companies, network service providers, and the information technology, finance, and aerospace industries. The group aims to develop recommendations to the President to assure vital telecommunications links through any event or crisis, and to help the U.S. government maintain a reliable, secure, and resilient national communications posture.

^bDHS, *National Response Framework* (Washington, D.C.: January 2008). The framework establishes a comprehensive, national, all-hazards approach to domestic incident response. It identifies the key response principles, as well as the roles and structures that organize national response. The document includes 23 Emergency Support Functions that provide the structure for coordinating federal interagency support for a federal response to an incident. Emergency Support Function 2 supports the restoration of the communications infrastructure, facilitates the recovery of systems and applications from cyber attacks, and coordinates federal communications support to response efforts during incidents requiring a coordinated federal response.

Under the National Infrastructure Protection Plan, DHS's Office of Cybersecurity and Communications, as the sector-specific agency for the communications and information technology sectors, is responsible for leading federal efforts to support sector protection efforts. As part of the risk management process for protecting the nation's critical infrastructure, including the protection of the cyber information infrastructure, the National Infrastructure Protection Plan recommends that outcome-oriented metrics be established that are specific and clear as to what they are measuring, practical or feasible in that needed data are available, built on objectively measureable data, and align to sector priorities. These

metrics are to be used to determine the health and effectiveness of sector efforts and help drive future investment and resource decisions.

DHS and its partners have previously identified the development of outcome-oriented metrics as part of the process to be used to manage risks to the nation's critical communications infrastructure. For example, in 2010, DHS and its communications sector partners identified preserving the overall health of the core network as the sector's first priority at the national level.²⁶ They also defined a process for developing outcome-oriented sector metrics that would map to their identified goals and would yield quantifiable information (when available). Additionally, DHS and its information technology sector partners stated that they would measure their cyber protection efforts related to DNS and BGP in terms of activities identified in 2009 to assist sector partners in mitigating risks to key sector services, such as providing DNS functionality and Internet routing services.²⁷ In 2010, they noted that implementation plans would be developed for each of the activities and outcome-based metrics would be used to monitor the status and effectiveness of the activities.²⁸

However, DHS and its partners have not yet developed outcome-based metrics related to the cyber-protection activities for the core and access networks, DNS functionality, and Internet routing services. For the communications sector, DHS officials stated that the sector had recently completed the first part of a multiphased risk assessment process that included identification of cyber risks. The officials further stated that efforts are under way to prioritize the identified risks and potentially develop actions to mitigate them. However, DHS officials stated that outcome-oriented metrics had not yet been established and acknowledged that time frames for developing such metrics had not been agreed to with their private sector partners. For the information technology sector, DHS officials noted that the information technology sector's private sector partners had decided to focus on progress-related metrics (which report the status of mitigation development activities as well as implementation decisions and progress) to measure the

²⁶DHS, *Communications Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan* (2010).

²⁷DHS, *Information Technology Sector Baseline Risk Assessment* (August 2009).

²⁸DHS, *Information Technology Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan* (2010).

effectiveness of sector activities to reduce risk across the entire sector and periodically re-examine their initial risk evaluation based on perceived threats facing the sector. While these progress-related metrics are part of the information technology sector’s planned measurement activities, the sector’s plans acknowledge that outcome-based metrics are preferable to demonstrate effectiveness of efforts.

Until metrics related to efforts to protect core and access networks, DNS, and BGP are fully developed, implemented, and tracked by DHS, federal decision makers will have less insight into the effectiveness of sector protection efforts.

| | |
|-----------------------|---|
| Department of Defense | Within DOD, the Office of the Chief Information Officer (CIO) has been assigned the responsibility for implementing Executive Order 13618 requirements related to NS/EP communication functions. As previously described, the CIO (along with the Assistant Secretary for Cybersecurity and Communications in DHS) co-chairs the NS/EP Communications Executive Committee established in Executive Order 13618. The CIO directs, manages, and provides policy guidance and oversight for DOD’s information and the information enterprise, including matters related to information technology, network defense, network operations, and cybersecurity. Table 5 describes the department’s efforts in relation to this executive order. |
|-----------------------|---|

Table 5: Department of Defense Key Efforts

| Component | Action |
|---|---|
| Office of the Chief Information Officer | Co-chairs the new Executive Committee for NS/EP Communications required by Executive Order 13618. Actions taken related to the executive committee include creating a charter for the committee (approved in September 2012), developing a staffing and resource plan for the Joint Program Office (in DHS), planning the specific tasks defined in the executive order, evaluating the current status and integration of existing efforts, and discussing how the dismantling of the National Communications System would impact NS/EP telecommunications functions. According to DOD officials, the executive committee is still in development and has not yet discussed cyber issues related to NS/EP communications. |

Source: GAO analysis of DOD data.

| | |
|------------------------|---|
| Department of Commerce | Federal law and policy also establish a role for the Department of Commerce (Commerce) related to the protection of the nation’s communications networks. For example, Commerce conducts industry studies assessing the capabilities of the nation’s industrial base to |
|------------------------|---|

support the national defense.²⁹ In addition, the department's National Telecommunications and Information Administration (NTIA) was established as the principal presidential adviser on telecommunications and information policies.³⁰ Further, Commerce's National Institute of Standards and Technology (NIST) is to, among other things, cooperate with other federal agencies, industry, and other private organizations in establishing standard practices, codes, specifications, and voluntary consensus standards.³¹

Commerce also has a role in ensuring the security and stability of DNS. Prompted by concerns regarding who has authority over DNS, along with the stability of the Internet as more commercial interests began to rely on it, the Clinton administration issued an electronic commerce report in July 1997 that identified the department as the lead agency to support private efforts to address Internet governance. In June 1998, NTIA issued a policy statement (known as the White Paper) that stated it would enter into an agreement with a not-for-profit corporation formed by private sector Internet stakeholders for the technical coordination of DNS.

In addition, Commerce created the Internet Policy Task Force in August 2011 to, among other things, develop and maintain department-wide policy proposals on a range of global issues that affect the Internet, including cybersecurity. While NIST has been identified as the Commerce lead bureau for cybersecurity, the task force is to leverage the expertise of other Commerce bureaus, such as the Bureau of Industry and Security and NTIA.³²

Commerce components also carry out functions related to the security of the nation's communications networks. The Bureau of Industry and

²⁹Executive Order No. 12656, *Assignment of Emergency Preparedness Responsibilities*, 53 Fed. Reg. 47491 (Nov. 23, 1988), and Executive Order No. 13603, *National Defense Resources Preparedness*, 77 Fed. Reg. 16651 (March 22, 2012), assign Commerce the responsibility to conduct industry studies.

³⁰47 U.S.C. § 902.

³¹15 U.S.C. § 272.

³²Other Commerce bureaus and offices identified as participants in the Internet Policy Task Force include the International Trade Administration, the Economics and Statistics Administration, the United States Patent and Trademark Office, and the Office of the Secretary.

Security conducted an industrial study to examine the operational and security practices employed by network operators in the nation's communications infrastructure. In addition, NTIA manages agreements with the Internet Corporation for Assigned Names and Numbers (ICANN) and VeriSign, Inc., through which changes are made to the authoritative root zone file.³³ Also, NIST participates in open, voluntary, industry-led, consensus-based, standards-setting bodies that design and develop specifications for network security technologies, including those used in the nation's communications networks (such as DNS and BGP) as well as in industry technical forums for the purpose of promulgating the deployment of such new technologies. Table 6 describes some of the key efforts of Commerce as they relate to the cybersecurity of the nation's communications networks.

Table 6: Department of Commerce Key Efforts

| Component | Action |
|---------------------------------|---|
| Bureau of Industry and Security | Conducted a national security assessment of the U.S. telecommunications infrastructure and its supply chains. Among other things, the survey's goal was to document network maintenance practices, understand issues affecting network reliability and integrity, and identify best practices to help ensure the operational reliability of the nation's critical information network infrastructure. Several questions in one of the two surveys conducted under the assessment asked telecommunications companies to identify how they protect components of their networks from cyber attack, as well as what the companies use to detect and analyze cyber threats and attacks. |
| Internet Policy Task Force | Issued a greenpaper, titled <i>Cybersecurity, Innovation and the Internet Economy</i> , which noted the need to promote existing industry-led development of standards, specifically identifying industry efforts related to DNS and BGP. ^a It also recommended that Commerce work with other government, private sector, and nongovernment organizations to proactively promote cybersecurity standards and practices. |

³³These agreements identify three roles for the authoritative process for managing changes to the root zone file. ICANN is the functions operator, which receives and processes root zone file change requests. VeriSign, Inc., is the root zone maintainer, which makes authorized root zone file edits and distributes the edited file to those who operate root zone servers. NTIA is the root zone administrator. NTIA's actions to fulfill its role and its interaction with ICANN and VeriSign, Inc., are described in table 6.

| Component | Action |
|---|---|
| National Telecommunications and Information Administration (NTIA) | <p>Reviews and authorizes changes to the DNS root zone file. Specifically, NTIA receives and processes root zone file change requests from ICANN. According to NTIA officials, this process includes a check to ensure that ICANN has complied with agreed upon verification and processing policies and procedures. NTIA then submits the authorized change request to VeriSign to edit the root zone file and distribute the changes.</p> <p>Performs oversight of the DNS root zone agreements. According to NTIA officials, this oversight includes reviewing ICANN security plans and audit reports, along with site visits.</p> <p>Oversees the implementation of DNSSEC in the DNS root zone. With assistance from NIST, NTIA contractually defined the baseline requirements for the root zone partners to implement DNSSEC across the root zone. NTIA receives monthly reports from the root zone partners indicating any planned or unforeseen events with respect to their DNSSEC operational and key management responsibilities.</p> <p>Contracted for additional security requirements (including an outage reporting requirement) in the latest version of the root zone contract, which went into effect October 2012.</p> |
| National Institute of Standards and Technology (NIST) | <p>Participates in industry-led working groups on DNS and BGP standards, such as the Internet Engineering Task Force Standards Development Organization and the North American Network Operators' Group. According to NIST officials, these efforts are undertaken in collaboration with DHS.</p> <p>Co-authored core DNSSEC standards issued by the Internet Engineering Task Force, as well as draft security standards for BGP.</p> <p>Develops and issues security standards and guidance for federal networks (including DNS and BGP). According to communications sector representatives, this guidance is widely used within the sector.</p> <p>Developed (in collaboration with DHS) an open-source rapid prototyping tool^b for early adopters of the BGP security standards. This prototype was presented to North American Network Operators Group participants for their consideration.</p> <p>Supports other federal organizations in carrying out their roles. For example, NIST assisted NTIA with developing the DNSSEC requirements for the root zone and supported the development of the Internet Policy Task Force greenpaper, <i>Cybersecurity, Innovation and the Internet Economy</i>.</p> <p>Serves as a member of the CSRIC board and participates in working groups related to DNS and BGP.</p> |

Source: GAO analysis of Commerce data.

^aInternet Policy Task Force, *Cybersecurity, Innovation and the Internet Economy* (June 2011).

^bSee http://www.nanog.org/meetings/nanog53/presentations/Monday/SRxAndBRITE_NANOG53.pdf.

Though Reporting Mechanisms Are in Place, FCC and DHS Have Not Received Reports of Cyber-Related Incidents Affecting the Nation's Core and Access Networks

No cyber incidents affecting the core and access networks have been reported by communications networks owners and operators through three established reporting mechanisms from January 2010 to October 2012.³⁴ To report incidents involving the core and access communications networks to the federal government, communication networks operators can use reporting mechanisms established by FCC and DHS to share information on outages and incidents:

- FCC's Network Outage Reporting System is a web-based filing system that communications providers use to submit detailed outage reports to FCC. In turn, FCC officials stated that the agency uses the reported outage data to develop situational awareness of commercial network performance as well as to aid the commission in influencing and developing best practices regarding incidents.
- DHS's Network Security Information Exchange is an information-sharing forum comprised of representatives from the communications and information technology sectors that meet bimonthly to voluntarily share communications-related incidents, among other things.
- DHS's National Cybersecurity and Communications Integration Center, which includes the National Coordinating Center, US-CERT, and the Industrial Control Systems Cyber Emergency Response Team, is used to share information about threats, vulnerabilities, and intrusions related to communications networks and the sector as a whole. Communications and information technology providers can voluntarily report threats, vulnerabilities, and intrusions to the center.

Although these mechanisms for reporting exist, available information showed that no cyber-based incidents involving the core and access communication networks had been reported using these mechanisms to the federal government from January 2010 to October 2012. Specifically, of the over 35,000 outages reported to FCC during this time period, none were related to traditional cyber threats (e.g., botnets, spyware, viruses,

³⁴Critical support components of the Internet have experienced cyber-related incidents. For example, cyber-based attacks on the DNS root servers occurred in 2002 and again in 2007. In the 2007 incident, at least 6 of the 13 root servers were subjected to a distributed denial-of-service attack. According to ICANN, although 2 of the root servers were badly affected, the attack had very limited impact on actual Internet users. In addition, there have been several public reports of cyber incidents related to BGP affecting networks inside the United States. These incidents involved erroneous routing data being propagated by foreign and domestic entities and, in what was described by a private sector security organization as an extremely rare occurrence, a spammer hijacking a foreign network to make it appear to be attached to a U.S. network.

and worms). FCC officials stated that there could be an increase in the presence of cyber-related outages reported in the future as the Voice-over-Internet-Protocol reporting requirements are enforced.³⁵ Further, DHS Office of Cybersecurity and Communications officials stated that no cyber incidents related to the core and access networks were reported to them during January 2010 to October 2012. For example, although several incidents attributed to the communications sector were reported to DHS's Industrial Control Systems Cyber Emergency Response Team in fiscal year 2012, none of these incidents involved core and access networks. Our review of reports published by information security firms and communication network companies also indicated that no cyber incidents related to the core and access networks were publicly reported from January 2010 to October 2012.

Officials within FCC and the private sector attributed the lack of incidents to the fact that the communications networks provide the medium for direct attacks on consumer, business, and government systems—and thus these networks are less likely to be targeted by a cyber attack themselves. In addition, Communications Information Sharing and Analysis Center officials expressed greater concern about physical threats (such as natural and man-made disasters, as well as unintentional man-made outages) to communications infrastructure than cyber threats.

³⁵On February 15, 2012, FCC extended outage reporting requirements to include interconnected Voice over Internet Protocol service. Providers are required to report significant network outages that meet specific criteria and thresholds. According to FCC announcement, this action was taken to make the nation's 9-1-1 systems more reliable and resilient.

Attributes of Defense Industry Cybersecurity Pilot Programs Could Be Applied to the Communications Sector

DOD, in its role as the sector-specific agency for the defense industrial base critical infrastructure sector,³⁶ established two pilot programs to enhance the cybersecurity of sector companies and better protect unclassified department data residing on those company networks. The Deputy Secretary of Defense established the Cyber Security/Information Assurance program under the department's Office of the Chief Information Officer to address the risk posed by cyber attacks against sector companies. The Opt-In Pilot was designed to build upon the Cyber Security/Information Assurance Program and, according to department officials, established a voluntary information-sharing process for the department to provide classified network security indicators to Internet service providers.³⁷

In August 2012, we reported on these pilot programs as part of our study to identify DOD and private sector efforts to protect the defense industrial base from cybersecurity threats. Our report described these programs in detail, including challenges to their success. For example, one challenge noted by defense industrial base company officials was that the quality of the threat indicators provided by the federal government as part of the Opt-In pilot had not met their needs. In addition, the quality of the pilot was affected by the lack of a mechanism for information sharing among government and private stakeholders. The report also made recommendations to DOD and DHS to better protect the defense industrial base from cyber threats. (The August 2012 report was designated as official use only and is not publicly available.)

Using information in that report, we identified six attributes that were implemented to varying extents as part of the pilot programs (see table 7).³⁸ These attributes were utilized by DOD and the defense industrial base companies to protect their sector from cyber threats and could inform the cyber protection efforts of the communications sector.

³⁶The defense industrial base critical infrastructure sector is described as the worldwide industrial complex that enables research and development, as well as design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts, to meet U.S. military requirements.

³⁷Network security indicators are information that is specific to identifying known or suspected cyber threats and may include data on Internet protocol addresses, domains, e-mail headers, files, and character strings.

³⁸The information from the August 2012 report used to identify the attributes was determined by DOD at that time not to be considered official use only.

Table 7: Relevant Attributes of the Defense Industrial Base Cyber Pilots

Agreements

Government sharing of unclassified and classified cyber threat information

Feedback mechanism on government services

Government cyber analysis, mitigation, and digital forensic support

Government reporting of voluntarily reported incidents

Internet service providers deploying countermeasures based on classified threat indicators for organizations

Source: GAO analysis of DOD and DHS data.

- **Agreements:** Eligible defense industrial base companies who wanted to participate in these pilots enter into an agreement with the federal government.³⁹ This agreement establishes the bilateral cyber-information-sharing process that emphasizes the sensitive, nonpublic nature of the information shared which must be protected from unauthorized use. The agreement does not obligate the participating company to change its information system environment or otherwise alter its normal conduct of cyber activities.
- **Government sharing of unclassified and classified cyber threat information:** DOD provides participating defense industrial base companies with both unclassified and classified threat information, and in return, the companies acknowledge receipt of threat information products. For any intrusions reported to DOD by the participating companies under the program, the department can develop damage assessment products, such as incident-specific and trend reports, and provide them to participating companies and DOD leadership.
- **Feedback mechanism on government services:** When a participating company receives cyber threat information from DOD, it has the

³⁹Currently, to be eligible to participate a defense industrial base company must (a) be capable of DOD-approved encrypted unclassified information sharing (with the government and defense industrial base participants); (b) have an active facility security clearance of Secret or higher; (c) have or acquire a communication security (COMSEC) account; (d) obtain access to DOD's Cyber Security/Information Assurance program secure voice and data transmission systems; (e) own or operate an information system that processes, stores, or transmits unclassified defense information; and (f) execute the framework agreement.

option of providing feedback to the department on, among other things, the quality of the products.

- Government cyber analysis, mitigation, and digital forensic support: A participating company can also optionally report intrusion events. When this occurs, DOD can conduct forensic cyber analysis and provide mitigation and digital forensic support. The department can also provide on-site support to the company that reported the intrusion.
- Government reporting of voluntarily reported incidents: In addition to providing cyber analysis, mitigation, and cyber forensic support, DOD can report the information to other federal stakeholders, law enforcement agencies, counterintelligence agencies, and the DOD program office that might have been affected.
- Internet service providers deploying countermeasures based on classified threat indicators for organizations: Each Cyber Security/Information Assurance program participating company can voluntarily allow its Internet service providers to deploy countermeasures on its behalf, provided the Internet service provider has been approved to receive classified network security indicators from the U.S. government. For those providers, US-CERT collects classified threat indicators from multiple sources and provides them to the companies' participating Internet service providers. If the Internet service provider identifies a cyber intrusion, it will alert the company that was the target of the intrusion. Providers can also voluntarily notify US-CERT about the incident, and US-CERT will share the information with DOD.

In May 2012, DOD issued an interim final rule to expand the Cyber Security/Information Assurance program to all eligible defense industrial base sector companies. Additionally, the Defense Industrial Base Opt-In Pilot became the Defense Industrial Base Enhanced Cybersecurity Service (DECS) Program, and is now jointly managed by DHS and DOD.⁴⁰

⁴⁰The Defense Industrial Base Enhanced Cybersecurity Services program is a component of the Joint Cybersecurity Services Program, which is managed by DHS's Office of Cybersecurity and Communications. DOD remains the point of contact for defense industrial base companies, while DHS works with Internet service providers.

In addition, on February 12, 2013, the President signed Executive Order 13636, which requires the Secretary of Homeland Security to establish procedures to expand DECS (referred to as the Enhanced Cybersecurity Services program) to all critical infrastructure sectors, including the communications sector. Considering these attributes and challenges could inform DHS's efforts as it develops these new procedures.

Conclusions

Securing the nation's networks is essential to ensuring reliable and effective communications within the United States. Within the roles prescribed for them by federal law and policy, the Federal Communications Commission and the Departments of Homeland Security, Defense, and Commerce have taken actions to support the communications and information technology sectors' efforts to secure the nation's communications networks from cyber attacks. However, until DHS and its sector partners develop appropriate outcome-oriented metrics, it will be difficult to gauge the effectiveness of efforts to protect the nation's core and access communications networks and critical support components of the Internet from cyber incidents. While no cyber incidents have been reported affecting the nation's core and access networks, communications networks operators can use reporting mechanisms established by FCC and DHS to share information on outages and incidents.

The pilot programs undertaken by DOD with its defense industrial base partners exhibit several attributes that could apply to the communications sector and help private sector entities more effectively secure the communications infrastructure they own and operate. As DHS develops procedures for expanding this program, considering these attributes could inform DHS's efforts.

Recommendation for Executive Action

To help assess efforts to secure communications networks and inform future investment and resource decisions, we recommend that the Secretary of Homeland Security direct the appropriate officials within DHS to collaborate with its public and private sector partners to develop, implement, and track sector outcome-oriented performance measures for cyber protection activities related to the nation's communications networks.

Agency Comments and Our Evaluation

We provided a draft of this report to the Departments of Commerce (including the Bureau of Industry and Security, NIST, and NTIA), Defense, and Homeland Security and FCC for their review and comment.

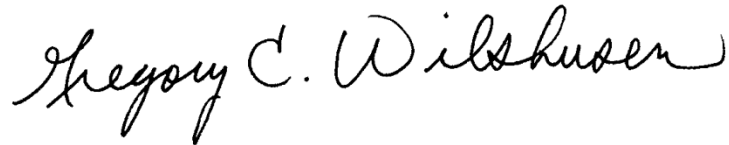
DHS provided written comments on our report (see app. II), signed by DHS's Director of Departmental GAO-OIG Liaison Office. In its comments, DHS concurred with our recommendation and stated that it is working with industry to develop plans for mitigating risks that will determine the path forward in developing outcome-oriented performance measures for cyber protection activities related to the nation's core and access communications networks. Although the department did not specify an estimated completion date for developing and implementing these measures, we believe the prompt implementation of our recommendation will assist DHS in assessing efforts to secure communication networks and inform future investment and resource decisions.

We also received technical comments via e-mail from officials responsible for cybersecurity efforts related to communication networks at Defense, DHS, FCC, and Commerce's Bureau of Industry and Security and NTIA. We incorporated these comments where appropriate.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 7 days from the report date. At that time, we will send copies to interested congressional committees; the Secretaries of the Departments of Commerce, Defense, and Homeland Security; the Chairman of the Federal Communications Commission; the Director of the Office of Management and Budget; and other interested parties. In addition, the report will be available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staff have any questions regarding this report, please contact me at (202) 512-6244 or at wilshuseng@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be

found on the last page of this report. Key contributors to this report are listed in appendix III.

A handwritten signature in black ink that reads "Gregory C. Wilshusen". The signature is written in a cursive style with a large, stylized 'G' and 'W'.

Gregory C. Wilshusen
Director
Information Security Issues

List of requesters

The Honorable Fred Upton
Chairman
The Honorable Henry Waxman
Ranking Member
Committee on Energy and Commerce
House of Representatives

The Honorable Greg Walden
Chairman
The Honorable Anna Eshoo
Ranking Member
Subcommittee on Communications and Technology
Committee on Energy and Commerce
House of Representatives

The Honorable Diana DeGette
Ranking Member
Subcommittee on Oversight and Investigations
Committee on Energy and Commerce
House of Representatives

Appendix I: Objectives, Scope, and Methodology

Our objectives were to (1) identify the roles of and actions taken by key federal entities to help protect the communications networks from cyber-based threats, (2) assess what is known about the extent to which cyber-incidents affecting the communications networks have been reported to the Federal Communications Commission (FCC) and Department of Homeland Security (DHS), and (3) determine if the Department of Defense's (DOD) pilot programs to promote cybersecurity in the defense industrial base can be used in the communications sector. Our audit focused on the core and access networks of the communication network. These networks include wireline, wireless, cable, and satellite. We did not address broadcast access networks because they are responsible for a smaller volume of traffic than other networks. Additionally, we focused on the Internet support components that are critical for delivering services: the Border Gateway Protocol (BGP) and Domain Name System (DNS).

To identify the roles of federal entities, we collected, reviewed, and analyzed relevant federal law, policy, regulation, and critical infrastructure protection-related strategies. Sources consulted include statutes such as the Communications Act of 1934, Homeland Security Act of 2002, and the Defense Production Act of 1950, as well as other public laws; the Code of Federal Regulations; National Communication System Directive 3-10; the National Infrastructure Protection Plan; the Communications Sector-Specific Plan; the Information Technology Sector-Specific Plan; the Communications Sector Risk Assessment; the Information Technology Sector Risk Assessment; Homeland Security Presidential Directives; selected executive orders; and related GAO products. Using these materials, we selected the Departments of Commerce, Defense, and Homeland Security, and FCC to review their respective roles and actions related to the security of the privately owned communications network because they were identified as having the most significant roles and organizations for addressing communications cybersecurity.

To identify the actions taken by federal entities we collected, reviewed, and analyzed relevant policies, plans, reports, and related performance metrics and interviewed officials at each of the four agencies. For example, we reviewed and analyzed Department of Commerce agreements detailing the process for how changes are to be made to the authoritative root zone file and Internet Policy Task Force reports on cybersecurity innovation and the Internet. In addition, we analyzed and identified current and planned actions outlined in DOD's National Security/Emergency Preparedness Executive Committee Charter. Also, we analyzed reports issued by the Communications Security, Reliability, and Interoperability Council on a variety of issues, including the security

of the Domain Name System and the Border Gateway Protocol. Further, we reviewed and analyzed the risk assessments and sector-specific plans for both the communications and information technology critical infrastructure sectors, as well DHS's plans for realignment in response to Executive Order 13618.

In addition, we interviewed agency officials regarding authority, roles, policies, and actions created by their department or agency, and actions taken by their departments and agencies to encourage or enhance the protection of communications networks, BGP, and DNS, and fulfill related roles. For Commerce, we interviewed officials from the Bureau of Industry and Security, National Telecommunications and Information Administration, and the National Institute of Standards and Technology. For DOD, we interviewed officials from the Office of the Chief Information Officer, including those from the National Leadership Command Capability Management Office and the Trusted Mission Systems and Networks Office. We also interviewed officials from the Office of the Under Secretary of Defense for Policy. For DHS, we interviewed officials from the National Protection and Programs Directorate's Office of Cybersecurity and Communications. For FCC, we interviewed officials from the International, Media, Public Safety and Homeland Security, Wireless Telecommunications, and Wireline Competition Bureaus. Based on our analysis and the information gathered through interviews, we created a list of actions taken by each agency. Additionally, we reviewed documents (including the communications sector risk assessment) from and conducted interviews with officials from the Communications Information Sharing and Analysis Center to assess federal efforts to fulfill roles and responsibilities.

To assess what is known about the extent to which cyber-incidents affecting the communications networks have been reported to FCC and DHS, we analyzed FCC policy and guidance related to its Network Outage Reporting System. Additionally, we conducted an analysis of outage reports submitted from January 2010 to October 2012 to determine the extent to which they were related to cybersecurity threats, such as botnets, spyware, viruses, and worms affecting the core and access networks. To assess the reliability of FCC outage reports, we (1) discussed data quality control procedures with agency officials, (2) reviewed relevant documentation, (3) performed testing for obvious problems with completeness or accuracy, and (4) reviewed related internal controls. We determined that the data were sufficiently reliable for the purposes of this report. We also interviewed officials from FCC's Public Safety and Homeland Security Bureau to understand incident

reporting practices of its regulated entities, and how reported incident data were used by FCC to encourage improvement or initiate enforcement actions. Further, we interviewed officials from DHS's United States Computer Emergency Readiness Team regarding the extent to which incidents were reported to it that affected core and access communications networks. We also conducted an analysis of information security reports from nonfederal entities, to determine if cyber incidents on the core and access communications networks had been reported to nonfederal entities. Additionally, we interviewed Communications Information Sharing and Analysis Center officials to identify the mechanisms and processes used to report cyber-related incidents in the communications sector to the center and then to the federal government.

To determine if DOD's pilot can be used to inform the communications sector, we reviewed our August 2012 report on DOD efforts to enhance the cybersecurity of the defense industrial base critical infrastructure sector.¹ We then identified and summarized attributes of the program that could be publicly reported and that were potentially applicable to the communications sector. The information used to compile the attributes from the August 2012 report was determined by DOD at that time not to be considered official use only. We also interviewed officials from DHS's Office of Cybersecurity and Communications to ascertain the current status of the pilot programs and efforts to determine the applicability of the pilots to all critical infrastructures, including the communications sector.

We conducted this performance audit from April 2012 to April 2013 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.

¹GAO, *Defense Cyber Efforts: Management Improvements Needed to Enhance Programs Protecting the Defense Industrial Base from Cyber Threats*, [GAO-12-762SU](#) (Washington, D.C.: Aug. 3, 2012). This report is restricted to official use only and is not publicly available.

Appendix II: Comments from the Department of Homeland Security

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



**Homeland
Security**

March 15, 2013

Mr. Gregory C. Wilshusen
Director, Information Security Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Wilshusen:

Re: Draft Report GAO-13-275, "COMMUNICATIONS NETWORKS: Outcome-Based Measures Would Assist DHS in Assessing Effectiveness of Cybersecurity Efforts"

Dear Mr. Wilshusen:

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

The Department is pleased to note GAO's acknowledgement of the variety of actions DHS has taken—in coordination with its communications sector partners—to develop a multi-phased risk assessment process that includes the identification of cyber risks. This process includes the development of outcome-oriented metrics as part of the overall process used to manage risks to the Nation's critical communications infrastructure.

The draft report contained one recommendation, with which the Department concurs. Specifically, GAO recommended that the Secretary of the Department of Homeland Security:

Recommendation: Direct the appropriate officials within DHS to engage all sector partners (federal and private) to develop, implement, and track the use of outcome-oriented performance measures for cyber protection activities related to the nation's communications networks.

Response: Concur. In September of 2012, DHS, in coordination with its public-private partnerships, finalized the 2012 National Sector Risk Assessment (NSRA) Report for Communications. DHS is currently working with industry to develop plans for mitigating risks identified in the NSRA. These plans will determine the path forward in developing outcome-oriented performance measures for cyber protection activities related to the Nation's core and access communications networks. The NSRA is just one example of the public-private partnership within the communications sector. Under Homeland Security Presidential Directive 7¹ (HSPD-7); Presidential Policy Directive 21², which supersedes HSPD-7; and the long-

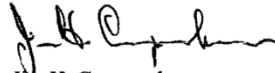
¹ Critical Infrastructure Identification, Prioritization, and Protection; December 17, 2003.

² Critical Infrastructure Security and Resilience; February 12, 2013.

standing operational relationship with the National Coordinating Center for Telecommunications, implementation of this recommendation is achievable. Working with owners and operators aligns with DHS's current plans to improve partnerships between government and industry, advance risk management, and increase information sharing. DHS's National Protection and Programs Directorate's Cybersecurity and Communication Stakeholder Engagement Office (Cyber Infrastructure Resilience Division) will lead this effort. Estimated Completion Date: To Be Determined.

Again, thank you for the opportunity to review and provide comments on this draft report. Technical comments were previously provided under separate cover. Please feel free to contact me if you have any questions. We look forward to working with you in the future.

Sincerely,



Jim H. Crumpacker
Director
Departmental GAO-OIG Liaison Office

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov

Staff Acknowledgments

GAO staff who made significant contributions to this report include Michael W. Gilmore, Assistant Director; Thomas E. Baril, Jr; Bradley W. Becker; Cortland Bradford; Penney Harwell Caramia; Kush K. Malhotra; Lee A. McCracken; David Plocher; and Adam Vodraska.

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 GAO's website (<http://www.gao.gov>). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to <http://www.gao.gov> and select "E-mail Updates."

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, <http://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 [E-mail Updates](#). Listen to our [Podcasts](#). Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: <http://www.gao.gov/fraudnet/fraudnet.htm>

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@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



Please Print on Recycled Paper.