United States Government Accountability Office

Report to the Committee on Armed Services, House of Representatives

March 2022

CYBERSECURITY

Internet Architecture Is Considered Resilient, but Federal Agencies Continue to Address Risks

GAO-22-104560

March 2022

CYBERSECURITY

Internet Architecture Is Considered Resilient, but Federal Agencies Continue to Address Risks

GAO Highlights

Highlights of GAO-22-104560, a report to the Committee on Armed Services, House of Representatives

Why GAO Did This Study

The internet is a global system of interconnected networks used by billions of people across the world to perform personal, educational, commercial, and governmental tasks. The U.S. government over time has relinquished its oversight role of the internet. A global, multistakeholder community made up of many organizations shapes internet policy, operations, and security. But the ongoing and increasing reliance on the internet underscores the need to understand the risks to its underlying architecture.

The House Committee on Armed Services Report accompanying the *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021* included a provision for GAO to examine internet architecture security. This report (1) identifies security risks related to the internet architecture and (2) determines the extent to which U.S. federal agencies have taken actions to address security risks to the internet architecture.

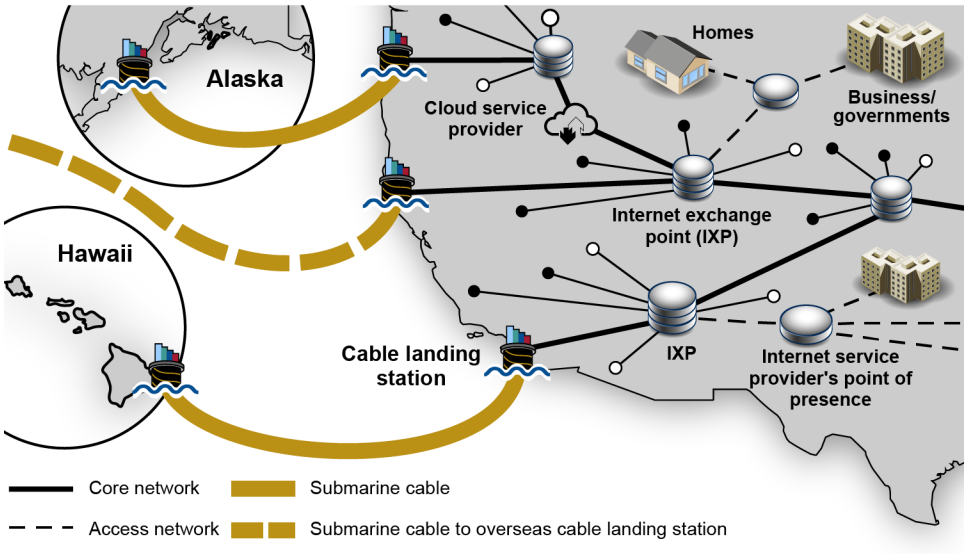
GAO collected and analyzed publicly available reports from federal and nonfederal organizations to identify risks to internet architecture components (internet exchange points, submarine cabling, the domain name system, and border gateway protocol, among others). GAO also reviewed federal law and policy and its prior work to identify federal internet architecture security roles and responsible agencies. Based on the agencies' roles, GAO collected and analyzed relevant documents and conducted interviews with officials from the responsible agencies.

View GAO-22-104560. For more information, contact David B. Hinchman at (214) 777-5719 or hinchmand@gao.gov.

What GAO Found

The communications sector operates the multiple, independent networks that form the basis for the internet. To support the exchange of network traffic, service providers manage and control core infrastructure elements with numerous components, including internet exchange points and submarine cable landing stations that connect to both domestic and international networks (see graphic). Multiple U.S. service providers operate distinct core networks that traverse the nation and interconnect with each other at several points.

How U.S. Internet Core Networks Connect to Service Providers



Source: GAO analysis of public and private sector reports. | GAO-22-104560

While experts consider the internet architecture to be resilient, it nevertheless faces a variety of cyber and physical risks that can impact its components; such risks can be intentional or unintentional (see table). In particular, cyber-related risks can impact two sets of protocols needed to ensure the uniqueness of names used in internet-based services and for facilitating the routing of data packets. Specifically, the domain name system translates names, such as www.gao.gov, to numerical addresses used by computers and other devices to route data. Additionally, the border gateway protocol is used to exchange network availability and routing information about individual networks (i.e., destinations). Both of these protocols are threatened by intentional abuse by malicious actors, as well as by unintentional failure. In addition, the internet architecture can be impacted by physical risks, such as cutting or removing fiber-optic cabling.

In addition, GAO convened two panels with subject matter experts. The panelists have experience in various aspects of the internet architecture, such as owning and operating elements of the infrastructure, participating in and contributing to standards setting organizations, and studying and participating in various multistakeholder governance entities.

During the panel sessions, GAO presented previously identified cyber and physical risks and requested that the experts identify additional risks or concerns that were not identified. GAO and the experts also discussed federal government involvement in addressing the risks.

Risks to Internet Architecture	
Cyber intentional	**Cyber unintentional**
• Denial-of-service attacks • Border gateway protocol (BGP) abuse • Domain name system (DNS) abuse • Supply chain exploitation • Malicious insider(s)	• BGP failures • DNS failures • Hardware failures • Software failures • Operator error
Physical intentional	**Physical unintentional**
• Intentional damage to fiber-optic cabling • Attack on an internet architecture facility or related infrastructure	• Accidental damage to fiber-optic cabling • Severe natural event

Source: GAO analysis of federal and nonfederal reports. | GAO-22-104560

Risks, if realized, may result in incidents that disrupt the proper functioning of the internet, including outages, degradation of performance, and interception of traffic. Panelists serving on two panels convened by GAO also stated that the risk of intentional incidents affecting the internet architecture depends on the capabilities and motives of malicious actors. GAO and others have reported on the threats posed by criminal groups and nation states, among others, which could potentially use their capabilities to impact components of the internet architecture. For example, a 2017 Department of Homeland Security information technology-related risk assessment identified organized crime and nation states as threats to operations providing domain name routing services.

As the U.S. government reduced its role regarding internet architecture components, including decommissioning early networks it had developed and relinquishing its oversight role of internet technical functions, those responsibilities passed to the global multistakeholder community. No one organization is responsible for the entirety of internet policy, operations, and security. However, the federal government fulfills a number of different roles that directly address risks to the internet architecture (see table). To fulfill these roles, agencies have taken actions. For example, DHS worked with members of the communications and information technology critical infrastructure sectors to, among other things, complete risk assessments on the sectors' ability to provide internet functions. In addition, the Federal Communications Commission impacts the security of the internet architecture through licensing submarine cables and landing stations, and administering a program to remove and replace equipment determined to pose an unacceptable risk to national security.

Federal Roles in Infrastructure Architecture Security
Guiding Critical Infrastructure Protection and Performing Private Sector Engagement
Engaging in International Cyber Diplomacy
Supporting Cyber Research and Development
Coordinating Cyber Incident Response
Investigating and Prosecuting Cyber Criminal Activity
Developing Security Standards
Regulating Portions of the U.S. Communication Network
Addressing Supply Chain Concerns Related to Data Routing Hardware and Services
Operating Domain Name System Root Zone Servers
Issuing Licenses to Land and Operate Submarine Cables

Source: GAO analysis of federal law and policy, agency documentation, and prior GAO reports. | GAO-22-104560

Contents

Abbreviations

ARL	Army Research Laboratory
BGP	border gateway protocol
CISA	Cybersecurity and Infrastructure Security Agency
DISA	Defense Information Systems Agency
DHS	Department of Homeland Security
DOD	Department of Defense
DOJ	Department of Justice
DNS	domain name system
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
NSF	National Science Foundation
NTIA	National Telecommunications and Information Administration
ODNI	Office of the Director of National Intelligence
PPD-41	Presidential Policy Directive 41

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

March 3, 2022

The Honorable Adam Smith
Chairman
The Honorable Mike Rogers
Ranking Member
Committee on Armed Services
House of Representatives

The internet has evolved from a research project involving four host computers in the 1960s to a vast global system of interconnected networks used by billions of people across the world to perform personal, educational, commercial, and governmental tasks.[1] The COVID-19 pandemic has highlighted the importance of internet access to communicate and conduct business via telework, telehealth, and distance learning. While the U.S. government has over time relinquished its oversight role of the internet to a global, multistakeholder community, the ongoing and increasing reliance on the internet underscores the need to understand the risks to its underlying architecture.[2]

The House Committee on Armed Services Report accompanying the *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021* includes a provision for GAO to provide a report examining internet architecture security.[3] In this report, our objectives were to (1) identify security risks related to the internet architecture and (2) determine the extent to which U.S. federal agencies have taken actions to address security risks to the internet architecture.

[1]According to the International Telecommunication Union (ITU), roughly 4.9 billion people were using the internet in 2021, an increase of approximately 782 million people since 2019.

[2]For the purposes of this report, "internet architecture" is defined in terms of select components that facilitate the transfer of data between connected high capacity networks. Specifically, these components are internet exchange points, high capacity cabling and information conduits, physical routing/switching infrastructure, border gateway protocol, and the domain name system. The term does not include any other components like certificate authorities, web standards, or any applications.

[3]H.R. Rep. No. 116-442, at 253-54 (2020) accompanying the *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021*, Pub. L. No. 116-283, 134 Stat. 3388 (2021).

To identify the cyber and physical security risks to the internet architecture, we collected and analyzed publicly available reports from federal and nonfederal organizations. We identified these reports through various sources, such as interviews with federal officials and keyword internet searches. We also used resources available from the National Academies of Sciences, Engineering, and Medicine to identify internet architecture subject matter experts and assembled two panels in June 2021.[4] The panelists have experience in various aspects of the internet architecture, such as owning and operating elements of the infrastructure, participating in and contributing to standards setting organizations, developing and maintaining network devices, researching security aspects of technical protocols, and participating in various multistakeholder governance entities. During each of the panel sessions, we discussed cyber and physical risks identified in GAO's analysis, as well as additional risks or concerns not previously identified.

To determine the extent to which U.S. federal agencies have taken actions to address security risks to the internet architecture, we reviewed federal law and policy and our prior work on internet governance and cybersecurity to identify existing cyber and physical security roles that have the potential to impact internet architecture components.[5] We determined that federal entity roles include, among others, guiding critical infrastructure protection, engaging in international partnership, supporting technology research and development, coordinating incident response, investigating and prosecuting criminal activity, developing security standards, and regulating aspects of the U.S. communication network.

Based on their roles, we identified 10 federal agencies to include in our review: the Departments of Commerce (Commerce), Defense (DOD), Homeland Security (DHS), Justice (DOJ), and State (State); the Federal Communications Commission (FCC); the National Science Foundation (NSF); the National Aeronautics and Space Administration (NASA); the Office of the Director of National Intelligence (ODNI); and the Office of

[4]The National Academies of Sciences, Engineering, and Medicine are private, nonprofit institutions that provide expert advice to help shape sound policies; inform public opinion; and advance the pursuit of science, engineering, and medicine.

[5]Prior reports we analyzed include: GAO, *Cybersecurity: Clarity of Leadership Urgently Needed to Fully Implement the National Strategy*, GAO-20-629 (Washington, D.C.: September 22, 2020); GAO, *Internet Management: Structured Evaluation Could Help Assess Proposed Transition of Key Domain Name and Other Technical Functions*, GAO-15-642 (Washington, D.C.: August 19, 2015); and GAO, *Communications Networks: Outcome-Based Measures Would Assist DHS in Assessing Effectiveness of Cybersecurity Efforts*, GAO-13-275 (Washington, D.C.: April 3, 2013).

Science and Technology Policy in the Executive Office of the President. We then conducted interviews with officials from these agencies and collected and analyzed evidence of actions taken to address these roles, including actions related to internet architecture security. The roles of federal agencies in protecting the internet architecture and how well each agency had performed in their role were also discussed with each of our subject matter expert panels, along with discussions on positive and negative impacts of the federal government in these roles. Observations raised by the subject matter experts included in the report were provided to the 10 selected federal agencies for comment. Appendix I has greater detail about our scope and methodology.

We conducted this performance audit from October 2020 to March 2022 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

The communications sector operates the multiple, independent networks that form the basis of the internet.[6] Public and private communications sector entities are responsible for, among other things, the use, architecture, and protection of their networks and associated services (including directing internet traffic). For example, private U.S. companies function as service providers that offer a variety of services to individual and enterprise end users or customers.

Of the multiple components of the nation's communications networks, the core networks are essential for internet functionality. The core networks transport a high volume of aggregated traffic over substantial distances and/or between different service providers or "carriers."[7] These networks achieve connectivity between regions within the United States using land-

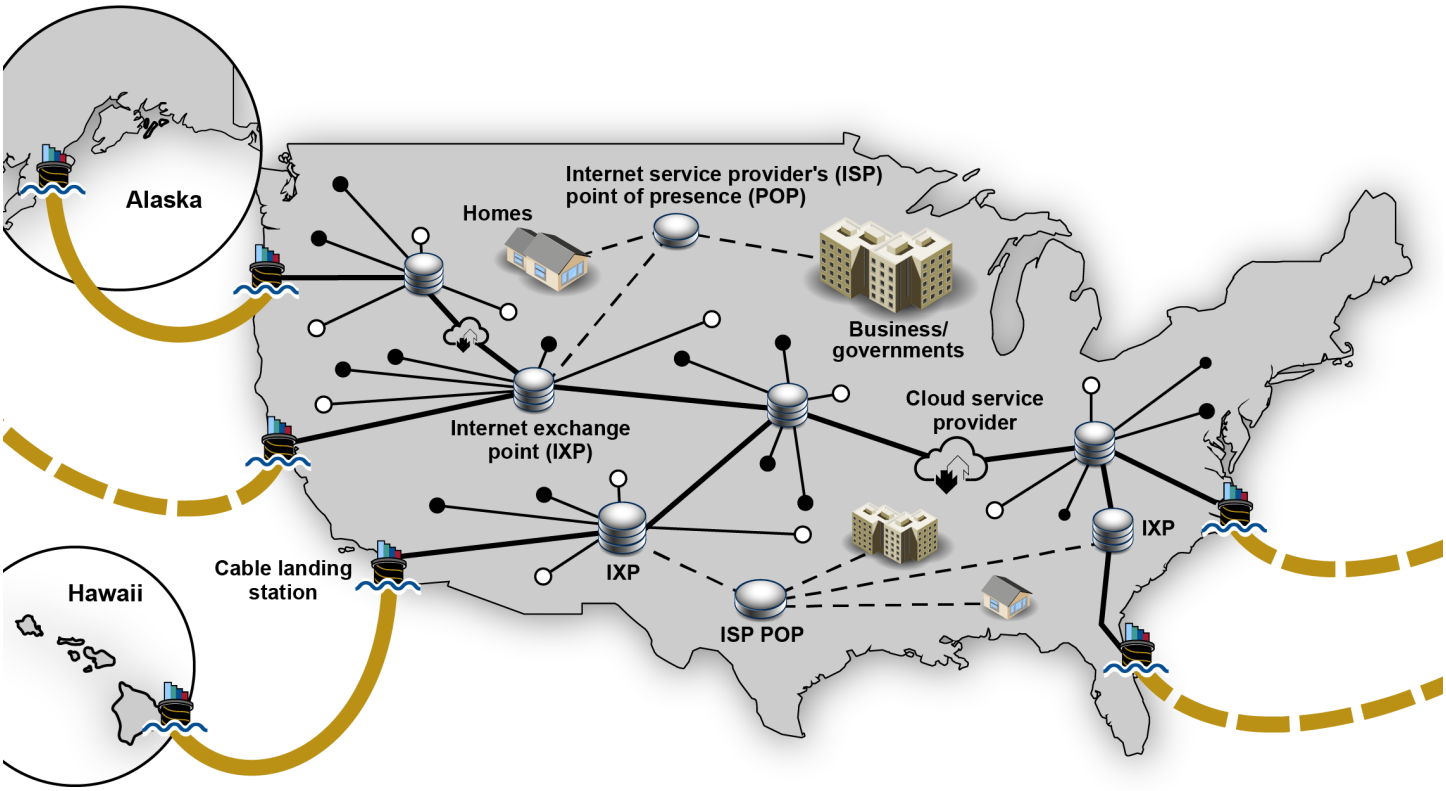
[6]Communications is one of 16 critical infrastructure sectors established by federal policy. The other sectors are chemical; commercial facilities; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; health care and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems. The communications sector delivers wired, wireless, and satellite communications to meet the needs of business and governments.

[7]Aggregate traffic is normally the multimedia (voice, data, video) traffic combined from different carriers to be transported over high speed through the core networks.

based fiber and coaxial cable networks and submarine fiber optic cable systems to connect distant places (i.e., Hawaii, Alaska, and U.S. territories) to the continental United States. In addition, these networks use submarine fiber optic cable systems to connect all the continents, except Antarctica, and other remote regions. According to FCC officials, international service providers also offer overseas connectivity to customers in the United States.

To support the exchange of network traffic, service providers manage and control core infrastructure elements with numerous components, including databases, switches, routers, internet exchange points, and operations centers. In addition, submarine cables come to shore at cable landing stations that connect to the core networks. Multiple U.S. service providers 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. Figure 1 depicts the path that internet traffic can take to its final destination.

Figure 1: How U.S. Internet Core Networks Connect to Service Providers



Source: GAO analysis of public and private sector reports. | GAO-22-104560

The U.S. government played a significant role in funding the development of the early internet, but over time reduced its role.[8] The Advanced Research Projects Agency provided funding to establish a research

[8]Details of the U.S. government's role in developing the internet can be found in appendix I of GAO, *Department of Commerce—Property Implications of Proposed Transition of U.S. Government Oversight of Key Internet Technical Functions,* B-327398 (Washington, D.C.: Sept. 12, 2016).

network beginning in the 1960s.[9] The resulting network was decommissioned in 1990. Following congressional authorization in 1992 to allow commercial activity on its backbone network and the increased network infrastructure development by commercial entities, the NSF decommissioned its network in 1995 and ended its direct role in developing internet infrastructure by 1998.[10]

In addition, the U.S. government relinquished its oversight role of the technical functions needed to make these systems run smoothly. In 1997, the President directed the Secretary of Commerce to move the governance of the domain name system (DNS) into the private sector to increase competition and promote international participation.[11] After Commerce's National Telecommunications and Information Administration (NTIA)[12] issued a 1998 policy statement,[13] the Internet Corporation for Assigned Names and Numbers (ICANN) was formed. ICANN is the nonprofit organization that manages the global coordination of DNS and other technical aspects underpinning the internet, known as the Internet Assigned Numbers Authority (IANA) functions. In March 2014, NTIA announced that if a suitable plan could be formed, it would finalize the transition of these internet technical functions to the multistakeholder community by letting its contract with ICANN expire, thus ending the U.S. government's role overseeing DNS. On October 1, 2016, the contract between ICANN and NTIA to perform these technical administrative functions expired, transitioning the coordination and

[9]The Advanced Research Projects Agency has changed its name to Defense Advanced Research Projects Agency.

[10]NSF's network, referred to NSFNET, came online in 1986 and grew to provide connection for other networks serving more than 4,000 research and educational institutions throughout the country. In 1991, NSF became responsible for coordinating and funding the management of the non-military portion of the internet infrastructure.

[11]The domain name system links email and website addresses with the underlying numerical addresses that computers use to communicate with each other.

[12]NTIA is the executive branch agency located within the Department of Commerce that is principally responsible for advising the President on telecommunications and information policy issues.

[13]This document is known as the domain name system "White Paper." See *Management of Internet Names and Addresses*, 63 Fed. Reg. 31741 (June 10, 1998). Prior to that, NTIA proposed that a private nonprofit entity, operated for the benefit of the internet as a whole, could coordinate the internet's technical functions, in a proposal known as the "Green Paper." See *Improvement of Technical Management of Internet Names and Addresses*, 63 Fed. Reg. 8826 (Feb. 20, 1998).

management of the internet's unique identifiers from the U.S. government to the private sector.[14]

Information Technology Sector Enables Internet Services through Products and Protocols

In conjunction with the communications sector, the information technology sector[15] provides the products (e.g., routers, switches, software, and operating systems) and protocols needed to provide internet routing, access, and connection service. Specifically, internet network operators employ voluntary, consensus standards called protocols to move data freely across communications networks. Two sets of protocols—DNS and the border gateway protocol (BGP)—are essential for ensuring the uniqueness of names used in internet-based services and for facilitating the routing of data packets, respectively.

DNS provides a globally distributed hierarchical database for mapping unique names, referred to as domain names, to network addresses. It translates domain names, such as www.gao.gov, into the numerical internet protocol addresses that computers and other devices use to route data across autonomous systems and back again.[16] This process relies on a hierarchical system of servers, called DNS servers, which store data linking domain 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 13 sets of root servers, which form a network of hundreds of servers that play a central role in the internet's system for finding a particular domain name. Each of these root DNS servers has a copy of a file called the authoritative root zone file, which is a type of "address book" for the top level (and only the top level) of the domain name system—listing, among other things, the internet protocol (IP) addresses of all top-level domains' name servers. This process can all take place within fractions of a second. Figure 2 shows an

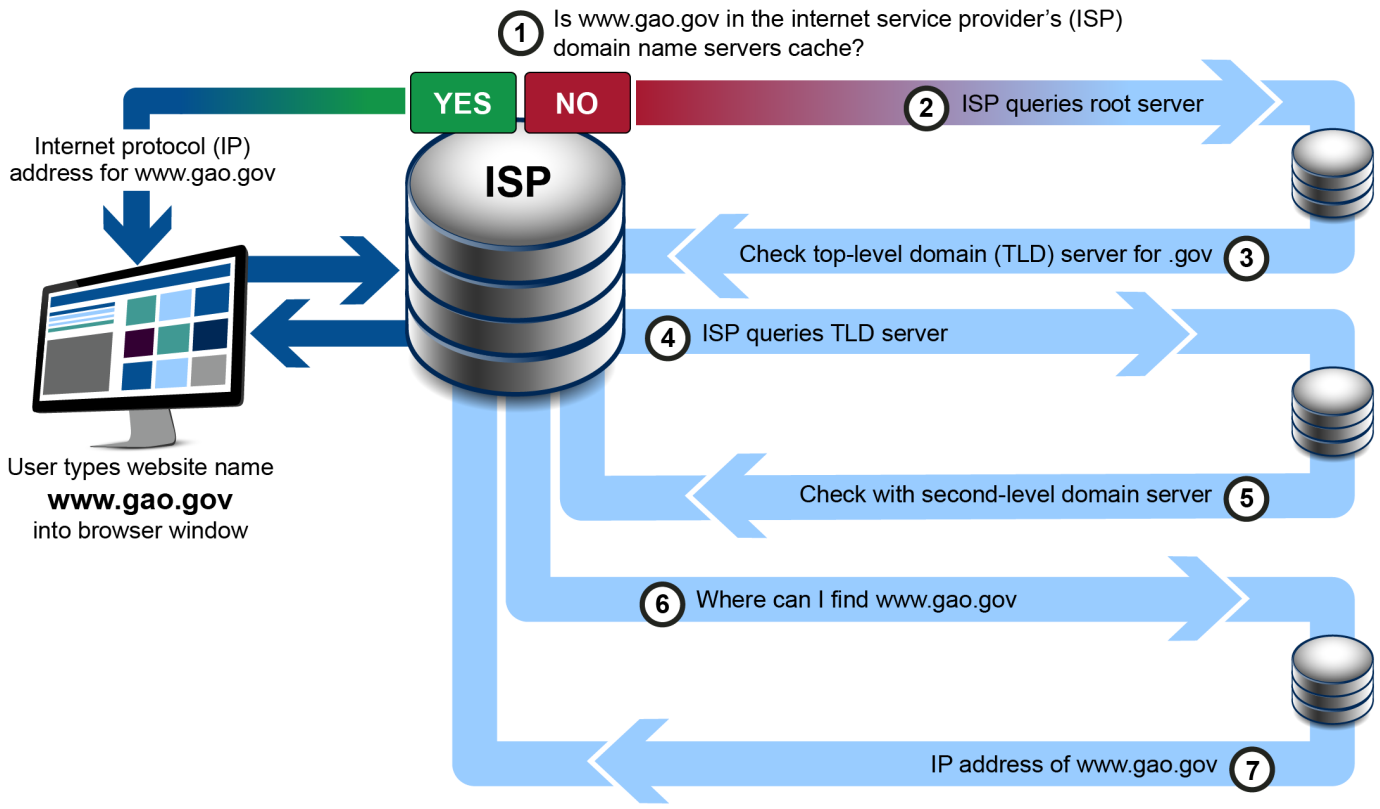
[14]Details of the U.S. government's decision to transition its internet oversight role to the multistakeholder community, and the potential implications of that transition, are set forth in B-327398, above.

[15]The information technology sector provides information technology, to include hardware manufacturers, software developers, and service providers, as well as the internet as a key resource.

[16]Autonomous systems are individual networks administered and operated by a single organization—such as that of a specific internet service provider or company.

example of this process for a user wanting to access www.gao.gov from their web browser.[17]

Figure 2: How the Domain Name System Uses the Authoritative Root Zone File to Direct an Internet Query



Source: GAO analysis of GAO and National Institute of Standards and Technology reports. | GAO-22-104560

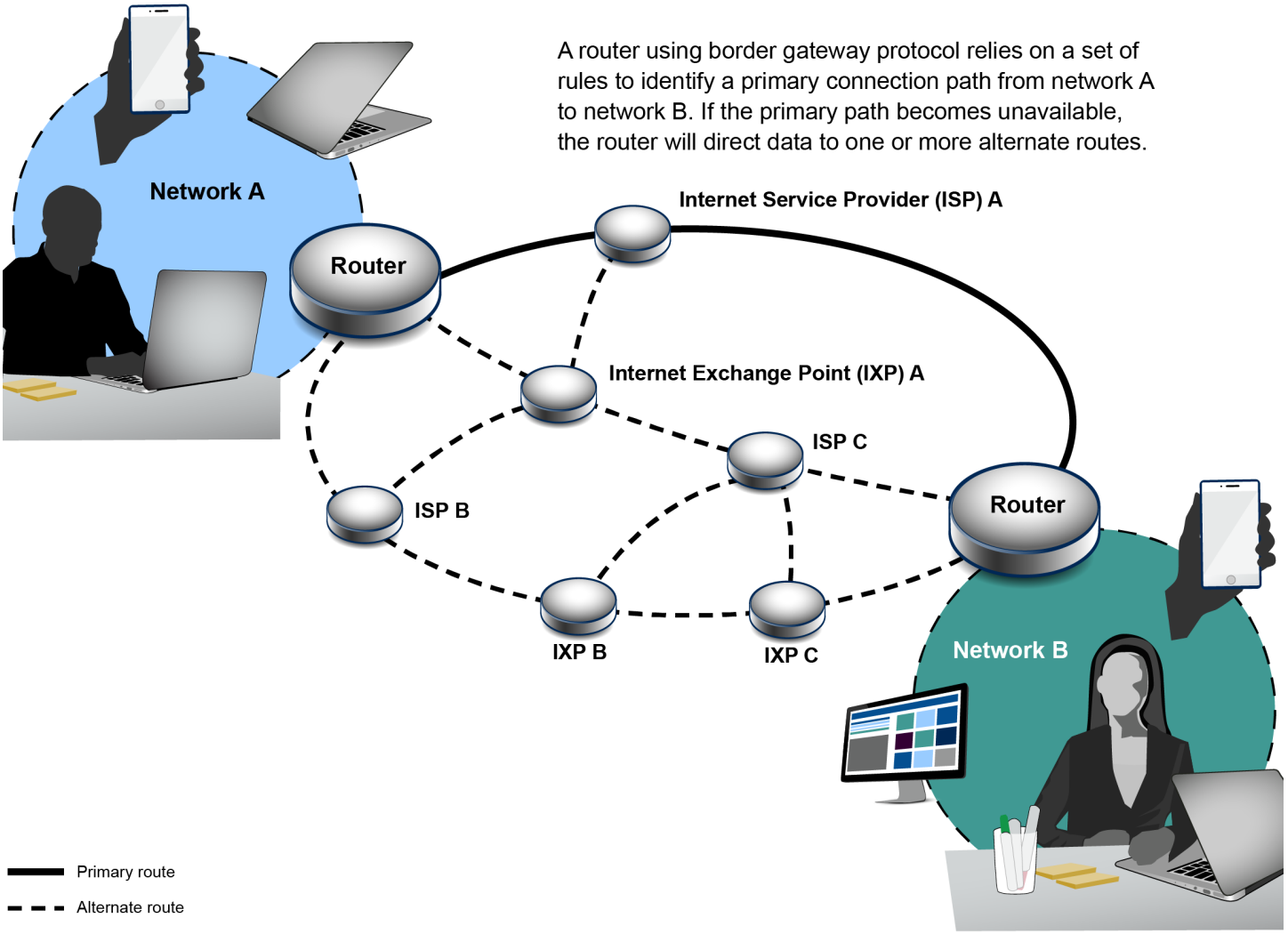
BGP is used by organizations connected to the internet to exchange network availability and routing information about individual networks (i.e. destinations). This information includes specific blocks of addresses that are reachable through a given organization and the list of networks that the traffic can pass through to reach its destination.[18] This protocol is

[17]For more information on the technical operation of DNS, see GAO-15-642.

[18]For more information on the technical specifics of BGP, see National Institute of Standards and Technology (NIST), *Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation*, Special Publication 800-189, (Gaithersburg, MD.: June 2019).

important because it binds together many autonomous networks that comprise the internet (see fig. 3).

Figure 3: Dynamic Routing Uses the Border Gateway Protocol



Source: GAO analysis of GAO and National Institute of Standards and Technology reports. | GAO-22-104560

Many Organizations Shape Internet Policy, Operations, and Security

No one organization is responsible for the entirety of internet policy and operations, including the security aspects of the internet's architecture. By design of the multistakeholder, global community, many public and private organizations and related processes have been formed that shape the internet's policy and operations (see table 1). The functions of these organizations that drive decisions about the internet's policy and operations and security include:

- developing technical standards
- managing resources for global naming and addressing capabilities
- providing network infrastructure services
- using the internet to communicate with each other and offer services and applications, or developing content, and
- educating and building capacity for developing and using internet technologies, such as multilateral organizations.

Table 1: Organizations That Shape Internet Policy, Operations, and Security

Organization	Role/Responsibility
Internet Engineering Task Force (IETF)	The IETF is an international community of network designers, operators, vendors, and researchers concerned with the evolution of the internet architecture and the smooth operation of the internet. It is the recognized international standards development organization for internet technologies and protocols, and open to any interested individual. http://www.ietf.org/
Internet Society (ISOC)	ISOC promotes the evolution and growth of the global internet through forums for open development of standards and protocols and international cooperation. Its members, chapters, and partners are a network of people and organizations that collaborate on policies supporting an open, globally connected, secure, and trustworthy internet. http://www.internetsociety.org/
Internet Architecture Board (IAB)	The IAB is chartered as a committee of the IETF and as an advisory body of the ISOC. Its responsibilities include, among other things, architectural oversight of IETF activities. The IAB is also responsible for the management of the IETF protocol parameter registries. http://www.iab.org/
Internet Research Task Force (IRTF)	The IRTF aims to create focused, long-term, and small research groups working on topics related to internet protocols, applications, architecture, and technology. http://www.irtf.org/
Internet Corporation for Assigned Names and Numbers (ICANN)	ICANN is a not-for-profit public-benefit corporation that is to promote competition and develop policy on the internet's unique identifiers through its coordination role of the internet's naming system. ICANN, through its affiliate Public Technical Identifiers, coordinates the system of unique names and numbers needed to keep the internet secure, stable, and interoperable. http://www.icann.org/

Organization	Role/Responsibility
Root Server System Advisory Committee (RSSAC)	RSSAC advises ICANN on matters relating to the operation, administration, security, and integrity of the Root Server System. The committee is comprised of operators who maintain the root name servers that are the apex of the Domain Name System. The operators include public and private sector organizations located around the world.
Internet Exchange Points (IXP)	Regional and national IXPs provide physical infrastructure that allows network operators to exchange internet traffic between their networks by means of mutual peering agreements.
Network Operators	Network operators include companies that provide access to the internet. Regional Network Operator Groups provide collaboration and consultative opportunities for local operators and among network operator groups globally.
Regional Internet Registries (RIRs)	RIRs oversee the allocation and registration of internet number resources within a particular region of the world. Each RIR is a member of the Number Resource Organization. RIRs include AfriNIC, the Asia Pacific Network Information Centre, the American Registry for Internet Numbers, the Latin American and Caribbean Internet Addresses Registry, and Réseaux IP Européens Network Coordination Centre. http://www.nro.net/
Universities and Academic Institutions	Academic institutions play a role in educating students and business people. They also prototype and demonstrate hardware and software solutions that benefit the internet, and carry out vulnerability research on software and applications supporting the internet architecture.
Other Standards Bodies	Many organizations focus on standards; some play roles in the internet. These organizations include the European Telecommunications Standards Institute, the Identity Commons, the Institute of Electrical and Electronics Engineers Standards Association, the International Organization for Standardization, the American National Standards Institute, the Liberty Alliance Project, Open Source Communities, and the Organization for the Advancement of Structured Information Standards.
Policy Discussion Forums	Additional organizations other than those mentioned specifically in the table, such as the Internet Governance Forum and the Organization for Economic Cooperation and Development, discuss internet governance issues with its members.

Source: GAO analysis of organization documentation. | GAO-22-104560

Internet policy and operations organizations have groups and activities that address security aspects of the internet architecture. For example, the Internet Engineering Task Force has multiple working groups formed to address information technology security topics, such as authentication,[19] encryption,[20] and network security. Standards-making organizations also address security including the Institute of Electrical and Electronics Engineers Standards Association that issues cybersecurity standards and hosts working groups on computer security and other information technology issues. Similarly, the Internet Architecture Board

[19]Authentication is the verification of the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

[20]Encryption is the transformation of data into a form that conceals the data's original meaning to prevent it from being known or used.

has established technical programs and administrative support groups to address internet-related technical and architectural considerations, such as DNS security and the security and stability of the routing system.

Federal policy emphasizes the importance of these organizations in internet architecture security. The 2018 National Cyber Strategy notes that the United States supports an open, interoperable, reliable, and secure internet through, among other things, participating in efforts to ensure the multistakeholder model of internet governance.[21] According to the strategy, this model is characterized by a transparent, bottom-up, consensus-driven process and enables governments, the private sector, civil society, academia, and the technical community to participate on equal footing, and helps deter attempts to create state-centric frameworks that could jeopardize the functionality of the internet.

While the Internet Architecture Is Considered Resilient, It Faces a Variety of Cyber and Physical Risks

Subject matter experts participating in the June 2021 panel discussions on the internet architecture and agency officials stated that the internet is a resilient system;[22] however, risks exist that threaten the internet architecture. In addition, incidents have occurred that impacted internet operations.

Panelists stated that owners and operators of internet components and services maintain internet functionality by building redundancy into the internet and actively addressing frequent issues with BGP, DNS, and hardware. Panelists also noted that unless a threat actor with the necessary capabilities, such as a nation state, intended to do more severe damage, the impacts of incidents related to the risks identified would typically be limited to specific regions or service providers.

Agency officials from DHS's Cybersecurity and Infrastructure Security Agency (CISA), DOD's Defense Information Systems Agency (DISA), and the Navy also noted the internet architecture's resiliency. For example, according to one Navy official, owners and operators of submarine cables

[21]The White House, *National Cyber Strategy of the United States of America* (Washington, D.C.: September 2018).

[22]The National Academies of Sciences, Engineering, and Medicine identified the subject matter experts. They have experience in various aspects of the internet architecture, including owning/operating elements of core network infrastructure, participating in and contributing to internet technology consensus-based standards setting organizations, developing/maintaining core network devices, researching security aspects of technical protocols that provide inter-autonomous system information exchange and evaluating, studying, and/or participating in various entities in the multistakeholder internet governance model.

that carry internet traffic ensure redundancy by connecting their cables to terrestrial networks in geographically diverse locations and using approaches that route traffic around cable failures. Further, DISA officials stated that the global DNS root zone system is resilient, and that domain resolution for the internet would continue to function even if one of the 13 logical root zone servers were to fail.

This resiliency is important, as the internet architecture faces a variety of cyber and physical risks. Various reports and expert panelists identified a number of cyber and physical risks that, if realized, could disrupt its proper functioning. These risks can be intentional, such as a malicious insider, or unintentional, such as a natural disaster. Table 2 categorizes the risks to internet architecture components identified in federal and nonfederal reports and in panel discussions with the subject matter experts.

Table 2: Risks to the Internet Architecture

Risk type	Risk category	Risk definition
Cyber intentional	Denial-of-service attacks	A denial-of-service attack against an internet architecture component prevents authorized access to resources or delays time-critical operations that support the functioning of the internet.
	Border gateway protocol (BGP) abuse	Exploitation of vulnerabilities in BGP protocol implementations or the trust inherent to the internet routing system itself.
	Domain name system (DNS) abuse	Exploitation of vulnerable DNS protocol implementations and configurations.
	Supply chain exploitation	Use of implants or vulnerabilities in a commercial IT product used by the target to access data or manipulate hardware, software, operating systems, peripherals, or services.
	Malicious insider(s)	An individual or group with authorized access (i.e., within the security domain) that has the potential to harm an information system or enterprise through destruction, disclosure, modification of data, and/or denial of service.
Cyber unintentional	BGP failures	Unintended events (e.g., traffic spikes, router misconfigurations) that disrupt the normal operation of global internet routing.
	DNS failures	Unintended events (e.g., traffic spikes, domain name collisions) that disrupt the normal operation of the DNS.
	Hardware failures	Unintended events (e.g., failure of environmental controls, electrical outages) that disrupt the normal operation of the physical infrastructure components the internet relies on.
	Software failures	Unintended events (e.g., software design flaws, incompatibilities) that disrupt the normal operation of the computer programs that support the internet architecture.

Risk type	Risk category	Risk definition
	Operator error	A technical mistake or lapse in judgement by an individual or organization that performs the operations of a system.
Physical intentional	Intentional damage to fiber-optic cabling	Malicious actors cutting, removing, or otherwise compromising fiber optic cables.
	Attack on an internet architecture facility or related infrastructure	Malicious actors causing physical damage (e.g., terrorist attacks) to physical internet architecture components, such as internet exchange points, root servers, and cable landing stations, or to other infrastructure relied upon to operate the internet, such as electric power.
Physical unintentional	Accidental damage to fiber-optic cabling	Events (e.g., a ship anchor dragging submarine cables, a backhoe digging up terrestrial cables, or high winds impacting aerial infrastructure) in which unintended contact with fiber optic cables cuts, tears, or otherwise compromises them.
	Severe natural event	Hurricanes, earthquakes, tsunamis, solar storms, and other natural events that damage physical internet architecture components, such as root servers and cable landing stations, or other infrastructure relied upon to operate the internet, such as electric power.

Source: GAO analysis of federal and nonfederal reports. | GAO-22-104560

During the June 2021 panel discussions, panelists emphasized the risk associated with supply chains that support the internet architecture. Specifically, panelists identified concerns about vulnerabilities built into networking components, disruption in the delivery of components, reliance on externally developed software code, and the lack of needed hardware components. In addition, panelists stated that entities lack visibility regarding these risks when purchasing components. Panelists also expressed concern about the trend toward centralization of internet services via cloud computing and the potential of this trend to create single points of failure, which could increase the impact of internet architecture security risks. Further, panelists stated that the risk of intentional incidents affecting the internet architecture depends on the capabilities and motives of malicious actors.

GAO and others have reported on the threats posed by criminal groups and nation states, among others, that have used their capabilities against public and private entities networks, applications, and operations that could potentially use their capabilities to affect components of the internet architecture. For example, in November 2021, we reported on the security threats to the communications sector and CISA's efforts to support that

sector.[23] Based on DHS's 2012 Risk Assessment Report for Communications, we reported that the Communications Sector faces serious physical, cyber-related, and human threats that could affect operations of local, regional, and national level networks.[24]

In addition, in September 2020, we reported[25] that there had been significant cyber-attacks conducted by advanced persistent threat groups on the financial services sector.[26] These resource-rich groups take direction from a nation state to steal information, disrupt operations, or destroy infrastructure. Further, a May 2017 risk assessment stated that subject matter experts supporting the information technology sector identified deliberate threats from organized crime and nation states, among others, related to various risks associated with providing domain name services.[27] The Office of the Director of National Intelligence similarly reported in April 2021 that foreign states use cyber operations to,

[23]GAO, *Critical Infrastructure Protection: CISA Should Assess the Effectiveness of its Actions to Support the Communications Sector*, GAO-22-104462 (Washington, D.C.: Nov. 23, 2021).

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

[25]GAO, *Critical Infrastructure Protection: Treasury Needs to Improve Tracking of Financial Sector Cybersecurity Risk Mitigation Efforts,* GAO-20-631 (Washington, D.C.: Sept.17, 2020).

[26]According to NIST, an advanced persistent threat can be an adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors, such as cyber, physical, and deception.

[27]Department of Homeland Security, *Provide Domain Name Resolution Services and Provide Internet Routing, Access, and Connection Services Critical Functions Risk Assessment* (Washington, D.C.: May 2017).

among other things, steal information and damage U.S. industry, including physical and digital critical infrastructure.[28]

Panelists also stressed that cyber risks to the internet architecture pose a greater threat than physical risks. They explained that cyber incidents can disrupt internet operations on a larger scale than physical incidents, which may only impact parts of the distributed, redundant infrastructure. Panelists also cited the relative difficulty in attributing cyber incidents to perpetrators and the strong protections around physical infrastructure as reasons they were more concerned about cyber incidents.

Past Cyber Incidents Disrupted Parts of the Internet Architecture

Cyber risks to the internet architecture, if realized, may result in intentional cyber incidents that cause outages, degrade internet performance, redirect or intercept traffic, or allow attackers to impersonate domains. These incidents include malicious actors conducting denial-of-service attacks, BGP abuse, DNS abuse, and supply chain attacks. Additionally, malicious insiders pose a risk to the internet architecture, as these insiders may abuse their access to internet architecture components to cause cyber incidents.

One example of an intentional cyber incident caused by malicious actors occurred in October 2016, when the actors used a botnet[29] comprised of infected Internet of Things devices to conduct a distributed denial-of-service attack against a major DNS provider.[30] The attack disabled websites and brought down the internet in some regions. The malware behind the attack searched the internet for unsecured devices, such as those that used factory-default usernames and passwords, and then used those devices to send junk DNS traffic to its targets until the targets could not function.

Cyber risks to the internet architecture, if realized, may also result in unintentional cyber incidents that cause outages, degrade internet performance, or redirect traffic to unintended locations. These incidents

[28]Office of the Director of National Intelligence, *Annual Threat Assessment of the US Intelligence Community* (Washington, D.C.: Apr. 9, 2021).

[29]A botnet is a network of devices infected with malicious software and controlled as a group without the device owners' knowledge.

[30]The President's National Security Telecommunications Advisory Committee, *NSTAC Report to the President on Internet and Communications Resilience* (Washington, D.C.: Nov. 16, 2017).

can result from BGP and DNS failures, hardware failures, software failures, and operator error.

Failures in BGP and DNS demonstrate the impact unintentional cyber incidents can have on the functioning of the internet:

- In June 2015, a misconfiguration caused a Malaysian telecommunications provider to make BGP announcements that indicated that the provider could receive traffic that it should not receive.[31] This incident redirected a large amount of internet traffic from all parts of the world to the telecommunications provider, resulting in global degradation of internet services for about 2 hours.
- In November 2018, a misconfiguration issue caused a Nigerian internet service provider to accidentally make BGP announcements that directed traffic intended for a large multinational technology company to a Chinese telecommunications provider.[32] The incident caused an outage of the technology company's services in many parts of the world for over 1 hour.
- In July 2021, a major DNS provider installed a software update that inadvertently triggered a bug in its DNS service, resulting in an outage of the service.[33] The outage reduced the availability of many websites and internet services. Internet users were unable to access these services for about 1 hour.

Physical Incidents Have Damaged Parts of the Internet Architecture

Physical risks to the internet architecture, if realized, may result in intentional physical incidents that cause outages or degrade internet performance. These incidents include malicious actors damaging or stealing fiber optic cabling or attacking internet architecture components like internet exchange points, root servers, or cable landing stations.

For example, in March 2007, a group of at least three ships stole sections of fiber optic cabling and optical amplifiers from the Thailand-Vietnam-Hong Kong and Asian Pacific Cable Network cable systems, taking over 3

[31]Andree Toonk, *Massive route leak cause Internet slowdown*, (June 12, 2015), accessed Sept.7, 2021, https://www.bgpmon.net/massive-route-leak-cause-internet-slowdown/.

[32]Ameet Naik, *Internet Vulnerability Takes Down Google*, (Nov. 12, 2018), accessed Sept. 7, 2021, https://www.thousandeyes.com/blog/internet-vulnerability-takes-down-google/.

[33]Mani Sundaram, *Akamai Summarizes Service Disruption*, (updated July 23, 2021), accessed Sept. 7, 2021, https://www.akamai.com/blog/news/akamai-summarizes-service-disruption-resolved.

months to repair.[34] The scale of the theft—involving approximately 177 kilometers of cabling and supporting equipment—exhausted the reserves of spare equipment the cable system operators kept on hand, slowing repair efforts. The incident reduced internet resiliency for countries in the region, and it was reported to cost an estimated $7.2 million to repair the cable systems.

More recently, in December 2020, a bomb detonated from inside a vehicle parked in downtown Nashville, Tennessee, near a network facility belonging to a major U.S. telecommunications company.[35] The explosion knocked out commercial power and destroyed infrastructure that linked to backup generators. The facility transitioned to temporary backup battery power, ensuring continuity in service immediately following the blast. When the batteries were depleted, however, communications service disruptions, including internet disruptions, occurred throughout the region. While national network traffic flowing through the Nashville hub automatically rerouted, traffic terminating or originating through this hub was impacted. Employees at the telecommunications company worked with federal, state, and local public safety agencies and officials to restore service, and most communications services were restored within 48 hours of the explosion.

Terrorist attacks can also impact the internet architecture. The September 11, 2001, attacks on the World Trade Center in New York City disrupted local communications infrastructure, including facilities, critical computer systems, and underground fiber-optic cables.[36] The attacks had a devastating effect on the regional communications infrastructure, which led to the closing of the financial markets for up to 1 week and interrupted internet connectivity to several universities, medical colleges, hospitals, and the city government's official website. The attacks also had unexpected impacts on the global internet, as some internet service providers in parts of Europe experienced outages and DNS disruptions occurred in South Africa due to interconnections in New York City. These disruptions to the global internet, however, were relatively minor, and

[34]Mick P. Green and Douglas R. Burnett, International Cable Protection Committee, Ltd., *Security of International Submarine Cable Infrastructure: Time to Rethink?* (2008, updated May 29, 2018).

[35]The President's National Security Telecommunications Advisory Committee, *NSTAC Report to the President on Communications Resiliency* (Washington, D.C.: May 6, 2021).

[36]GAO, *Internet Infrastructure: DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan*, GAO-06-672 (Washington, D.C.: June 16, 2006).

internet functionality outside of the New York area was largely back to normal within 15 minutes.

Physical risks to the internet architecture, if realized, may also result in unintentional physical incidents that cause outages or degrade internet performance. These incidents include damage to fiber-optic cabling from construction, accidents, and severe natural events such as hurricanes and earthquakes. For example, in 2003, six submarine cables were damaged off the coast of Algeria following an earthquake, disrupting all submarine networks in the Mediterranean region.[37] Additionally, when Hurricane Katrina made landfall in Louisiana in August 2005, it significantly damaged or destroyed the communications infrastructure in Louisiana, Mississippi, and Alabama.[38] The damage led to a loss of routing around the affected area, but it did not have a significant impact on global internet routing. Further, in January 2022, Tonga lost internet connection when a volcanic eruption damaged a fiber-optic cable.[39]

Agencies Fulfill a Number of Roles That Address Internet Architecture Security Risks

As previously discussed, over time the U.S. government reduced its role regarding internet architecture components, including decommissioning early networks it had developed and relinquishing its oversight role of internet architecture technical functions. Those responsibilities passed to the global multistakeholder community. No one organization is responsible for the entirety of internet policy, operations, and security.

Nevertheless, the federal government has a number of different roles that directly address risks to the internet architecture, such as those risks discussed earlier in this report. Specifically, federal law and policy establish various roles for federal agencies related to, among other things, critical infrastructure protection, international partnership engagement, cyber research and development, cyber incident response, and criminal investigation. To fulfill these roles, agencies have taken actions such as disseminating threat information and contributing to multistakeholder internet governance groups. In addition, federal agencies actively play specific roles that impact the security of the internet architecture. These activities include administering the removal

[37]Lionel Carter, Douglas Burnett et al, *Submarine cables and the oceans: connecting the world*, (Jan. 2009).

[38]GAO-06-672.

[39]Government of Tonga, *First Official Update Following the Volcanic Eruption,* press release (Jan. 18, 2022). Accessed Feb. 23, 2022: https://www.gov.to/press-release/first-official-update-following-the-volcanic-eruption/

and replacement of untrusted equipment and services, operating and securing three of the 13 logical root zone servers, and licensing submarine cables and associated cable landing stations.

Table 3 summarizes these roles and the federal agencies that have associated internet architecture security responsibilities. Agencies' actions related to these roles are discussed in greater detail below.

Table 3: Federal Roles in Internet Architecture Cyber and Physical Security

Roles	Agencies
Guiding Critical Infrastructure Protection and Performing Private Sector Engagement	Cybersecurity and Infrastructure Security Agency
	Federal Communications Commission
	National Telecommunications and Information Administration
Engaging in International Cyber Diplomacy	Department of State
	National Telecommunications and Information Administration
	Federal Bureau of Investigation
	Federal Communications Commission
Supporting Cyber Research and Development	Office of Science and Technology Policy
	National Institute of Standards and Technology
	National Science Foundation
Coordinating Cyber Incident Response	Cybersecurity and Infrastructure Security Agency
	Federal Bureau of Investigation
	Office of the Director of National Intelligence
Investigating and Prosecuting Cyber Criminal Activity	Department of Justice
	Federal Bureau of Investigation
	U.S. Coast Guard
Developing Security Standards	National Institute of Standards and Technology
Regulating Portions of the U.S. Communication Network	Federal Communications Commission
Addressing Supply Chain Concerns Related to Data Routing Hardware and Services	Federal Communications Commission
	National Telecommunications and Information Administration
Operating Domain Name System Root Zone Servers	Defense Information Systems Agency
	Army Research Lab
	National Aeronautics and Space Administration
Issuing Licenses to Land and Operate Submarine Cables	Federal Communications Commission

Source: GAO analysis of federal law and policy, agency documentation, and prior GAO reports. | GAO-22-104560

Federal Agencies Guide Critical Infrastructure Protection and Perform Private Sector Engagement

Federal law, policy, plans, and strategies establish oversight roles and responsibilities for the protection of the nation's critical infrastructure. Specifically, the *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021,* Presidential Policy Directive 21 *(Critical Infrastructure Security and Resilience),* the *National Infrastructure Protection Plan,*[40] and the National Cyber Strategy, identify ways federal agencies may work with the private sector to manage risks to protect the nation's critical infrastructure.[41] Federal agencies identified as sector risk management agencies are responsible for providing institutional knowledge and specialized expertise for securing the nation's critical infrastructure. These agencies are responsible for leading, facilitating, or supporting infrastructure protection activities, against all hazards, in their designated critical infrastructure sector.

DHS delegated its sector risk management agency responsibilities to CISA, which was designated by the *Cybersecurity and Infrastructure Security Agency Act of 2018,* for the two sectors responsible for internet architecture components—communications and information technology.[42] In this role, CISA has taken several actions related to internet architecture security, including

- completing, in May 2017, an updated risk assessment on the ability of the sectors to provide DNS and internet routing functions in coordination with government and private sector stakeholders;
- identifying threats such as DNS attacks, BGP route leaks, and hardware compromises in the CISA-led Information and

[40]*William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021,* Pub. L. No. 116-283, § 9002(c), 134 Stat. 3388, 4770 (2021); the White House, *Critical Infrastructure Security and Resilience*, Presidential Policy Directive/PPD-21: (Washington, D.C.: Feb. 12, 2013); Department of Homeland Security, *National Infrastructure Protection Plan, NIPP 2013: Partnering for Critical Infrastructure Security and Resilience* (December 2013); The White House, *National Cyber Strategy of the United States of America* (September 2018).

[41]The term "critical infrastructure," as defined in the *Critical Infrastructures Protection Act of 2001*, refers to systems and assets so vital to the United States that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these. 42 U.S.C. § 5195c(e).

[42]*Cybersecurity and Infrastructure Security Agency Act of 2018*, Pub. L. No. 115-278, § 2(a), 132 Stat. 4168 (2018) (codified at 6 U.S.C. § 652). The act assigned CISA the responsibility to enhance the security of the nation's critical infrastructures in the face of both physical and cyber threats.

Communications Technology Supply Chain Risk Management Task Force's threat scenario report;[43]

- conducting assessments of submarine cable systems, internet backbone links, and information technology organizations associated with network hardware production and internet routing, access, and connections, according to CISA officials; and
- using analytic tools, such as the Infrastructure Mapping Tool and Undersea Cable Infrastructure Tool, to evaluate regional internet infrastructures.

In addition, according to CISA officials, they plan to identify systems, assets, and critical technologies that enable core networks operation and internet-related services.[44]

While CISA has the lead role as the sector risk management agency, additional federal agencies also engage with the private sector on internet architecture security related issues. Specifically, several iterations of the Communications Security, Reliability and Interoperability Council (CSRIC)—a federal advisory committee chartered and administered by FCC composed of private and public communications stakeholders—developed reports on internet architecture security issues. These issues included cybersecurity risk management for communications sector segments (including internet backbone providers) and clustering of submarine cables and cable landing stations.[45] The reports contained recommendations to the FCC and resources for the communications sector. According to FCC officials, the recommendations led to further examination of FCC's activities and additional engagement with other agencies.

[43]CISA, Information and Communications Technology Supply Chain Risk Management Task Force, *Threat Evaluation Working Group, Supplier, Products, and Services Threat Evaluation (to include Impact Analysis and Mitigation),* Version 3.0 (July 2021).

[44]According to CISA officials, this is part of CISA's efforts related to National Critical Functions. National Critical Functions are functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

[45]See, for example, CSRIC IV, Cybersecurity Risk Management and Best Practices Working Group 4, *Final Report* (March 2015) and CSRIC V, Working Group 4A, *Submarine Cable Resiliency Final Report—Clustering of Cables and Cable Landings* (September 2016).

In addition, Commerce's NTIA works with the private sector to find consensus around shared solutions to cybersecurity marketplace challenges, including risks to internet architecture components. Our June 2021 panelists stated NTIA engages with private sector entities involved in the operation of the internet and represents those entities' interests in the interagency process.

International Engagement Results from Cyber Diplomacy Efforts

Several federal agencies conduct international engagement as part of cyber diplomacy efforts. This engagement is to help the United States promote the multistakeholder approach to internet governance and foster adherence to the established norms of responsible state behavior in cyberspace.

The U.S. Department of State leads the federal government's cybersecurity diplomacy efforts with international partners, and includes aspects of internet architecture security as part of these efforts. For example, pursuant to Executive Order 13800,[46] State worked with other federal agencies to develop an international engagement strategy on cybersecurity, which, among other things, addresses approaches that countries and stakeholders can take to manage internet architecture security risks.[47] The strategy calls for the United States to promote the role of non-government stakeholders in the existing multistakeholder internet governance system. It also calls for the United States to advance an international regulatory environment that supports innovation and respects the global nature of cyberspace by encouraging private sector innovation to address security risks across the digital ecosystem.

Further, according to State officials, the department actively worked on developing the March 2021 consensus report from the United Nations Open Ended Working Group and the July 2021 consensus report of the United Nations Group of Governmental Experts on Advancing

[46]The White House, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, Executive Order 13800 (Washington, D.C.: May 11, 2017).

[47]Department of State, Office of the Coordinator for Cyber Issues. *Recommendations to the President on Protecting American Cyber Interests through International Engagement* (Washington, D.C.: May 31, 2018).

Responsible State Behavior in Cyberspace.[48] The reports noted the growing concern about malicious activities that impact information and communications technologies, and signatories to the report agreed that nations should endeavor to ensure the general availability and integrity of the internet.

Additional cyber-related diplomacy efforts cited by State officials include contributions to the Internet Governance Forum, the Internet Engineering Task Force, the Institute of Electrical and Electronics Engineers, and the Organization for Economic Cooperation and Development, among other organizations and forums. State officials also stated they coordinate with other federal agencies on their international outreach.

In addition to State's leadership role, Commerce contributes to international engagement and includes internet architecture security as part of its activities. Specifically, within Commerce, NTIA's Office of International Affairs contributes to international engagement on internet architecture security. The office is the U.S. representative on the Government Advisory Committee at ICANN, and involves other U.S. federal agencies to help fulfill this role.

According to NTIA officials, the Office of International Affairs receives reports from ICANN and distributes these reports to the DNS interagency working group for input from other federal agencies. NTIA officials stated that members of the working group represent, among other organizations, DHS, DOD, DOJ, NASA, National Institute of Standards and Technology (NIST), and State. NTIA officials added that feedback from the working group informs the positions NTIA advances in the Government Advisory Committee meetings.

The Office of International Affairs also assists the State Department in its activities at the Internet Governance Forum and the International

[48]United Nations General Assembly, *Final Substantive Report of the Open-ended working group on developments in the field of information and telecommunications in the context of international security*, A/AC.290/2021.CRP.2 (Mar. 10, 2021). United Nations General Assembly, *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, A/76/135 (July 14, 2021).

Telecommunication Union (ITU).[49] According to NTIA officials, NTIA representatives attend Internet Governance Forum meetings to advocate for the current multistakeholder approach to internet governance; open, interoperable communications; and U.S. positions on topics such as emerging technologies. In addition, at the ITU, NTIA officials have been building a coalition to work against models for the internet architecture that may offer authoritarian governments more control over the internet.

Further, officials from other agencies noted international engagement efforts on internet architecture security. Federal Bureau of Investigation (FBI) officials stated that in the past 2 years, there were bureau representatives in the United States delegation to multiple ITU working groups, as well as presenting at and participating in Internet Governance Forum meetings. FCC officials also stated that they were active at the ITU, the Organization of American States' Inter-American Telecommunication Commission, and bilateral discussion with international partners.

Federally Sponsored Cyber Research and Development Support Internet Architecture Security

Federal agencies have a role in coordinating federally sponsored research and development in support of infrastructure protection and funds for cybersecurity research projects. The Office of Science and Technology Policy, NSF, and Commerce have activities within their organizations' cybersecurity research and development roles that address internet architecture security. For example, according to program documentation, the Office of Science and Technology Policy's Networking and Information Technology Research and Development (NITRD) Program coordinates the IT research and development and technology-transfer activities of 23 federal member agencies and about 50 other participating agencies. Within NITRD, there are two interagency working groups—one on large scale networking, and another on cyber security and information assurance—that coordinate on aspects of the internet architecture. The aspects include the security of the core network and the IT components in computing and communications systems.

NSF directorates also fund research and development activities related to internet architecture components under existing cybersecurity programs.

[49]The International Telecommunication Union is a United Nations specialized organization that regularly convenes specialists drawn from industry, the public sector, and research and development entities worldwide. The purpose is to develop technical specifications that are to ensure that each piece of the communications systems can interoperate seamlessly with the myriad elements that make up today's information and communications technology networks and services.

Specifically, NSF's Secure and Trustworthy Cyberspace program and Formal Methods in the Field program have funded several projects on DNS and BGP security, including projects related to DNS abuse, BGP abuse, and legal issues related to implementing secure routing architecture. NSF staff also identified a prior program called Future Internet Architectures, and stated that every funded project under the program focused on inherently secure clean-slate architectures and architectural components.

Further, according to NIST officials, it conducts research in threat analysis and problem definition, design of novel solution techniques, modeling and analysis of early designs, rapid prototyping of emerging specifications, and test and measurement of early implementations and deployments. NIST officials identified ongoing projects focused on various issues in internet architecture protection, including BGP security and resilience, DNS security, DNS abuse mitigation, and software defined security architectures. NIST officials identified specific examples of BGP activities:

- leading the development of a consensus problem definition for BGP route leaks;
- researching the application of artificial intelligence techniques to identify and mitigate route leaks;
- modeling and analysis of the performance impact of proposed BGP security solutions;
- developing rapid prototypes of emerging BGP security specifications;
- developing test and measurement tools to assist early implementers and adopters of BGP security solutions; and
- developing deployment guidance, technology demonstrations and practice guides to foster operational deployment of BGP security.

Federal Agencies Coordinate the Response to Security-related Incidents

Presidential Policy Directive (PPD) 41, issued in July 2016, sets forth principles governing the federal government's response to cyber incidents involving government or private sector entities, and establishes the

process to form a Cyber Unified Coordination Group.[50] According to CISA officials, the process set out in PPD-41 has not been utilized for incidents impacting internet architecture security.

However, in August 2020, CISA led a national cyber incident response exercise that contained a scenario involving DNS and BGP.[51] Participants in the exercise included federal agencies such as Commerce, DHS, and FCC, as well as nonfederal representatives from the Information Technology critical infrastructure sector, among others. According to the exercises' after-action report, participants examined the process necessary to convene a Cyber Unified Coordination Group, as defined in PPD-41, and engaged in interagency discussions.

Our June 2021 panelists discussed the importance of incident response activities. Panelists specifically mentioned conducting incident exercises to help response teams gain experience before an incident occurs, and noted that the federal government could help conduct incident response activities in a professional manner. Panelists also discussed the importance of after action reporting for any incident, although panelists cautioned that there are cultural and legal issues associated with sharing these reports with external entities.

ODNI also is involved in internet architecture security. According to ODNI officials, ODNI shares threat intelligence information, identifies risks to infrastructure including submarine cables, and coordinates with the FBI and DHS to collaborate on the government response to significant cyber incidents. ODNI officials also stated that more specific ODNI activities relative to internet architecture security would be classified and too sensitive for a public report.

[50]The White House, *United States Cyber Incident Coordination*, Presidential Policy Directive/PPD-41 (Washington, D.C.: July 26, 2016). In response to significant cyber incidents, this PPD establishes the Cyber Unified Coordination Group as the primary method of coordinating between federal agencies. The directive instructs federal lead agencies to undertake three concurrent lines of effort: threat response, led by DOJ acting through the FBI; asset response, led by DHS acting through CISA; and intelligence support and related activities, led by the Office of the Director of National Intelligence. Sector risk management agencies will be included in a Cyber Unified Coordination Group if an incident affects their sectors.

[51]The exercise was part of Cyber Storm, a series of exercises to improve the nation's cybersecurity readiness, protection, and incident response capabilities.

According to a Navy official with submarine cable responsibilities, the Navy and the Military Sealift Command are working with the Department of Transportation's Maritime Administration to establish a fleet of cable repair ships as first responders to be responsive at the federal government's direction. The fleet shall be retained under operating agreements as required by the *National Defense Authorization Act for Fiscal Year 2020*.[52] The official also stated that the Cable Security Fleet would provide emergency cable repairs on commercially-owned assets when other repair ships are not available or able to respond or unwilling to respond and, most likely, when the owners request government assistance with repairs.

Law Enforcement Agencies Investigate and Prosecute Criminal Activity

Federal agencies investigate physical and cyber-related incidents on critical infrastructure. Further, federal efforts involve conducting law enforcement investigations of possible violations of federal laws. The Department of Justice (DOJ), FBI, and U.S. Coast Guard engage in criminal investigation and law enforcement activities in accordance with their missions to defend U.S. interests, ensure safety against foreign and domestic threats, and provide federal leadership in preventing and controlling crime targeting the nation's cyber infrastructure. Specifically, DOJ officials stated that the Criminal Division implements DOJ national strategies to combat computer and intellectual property crimes worldwide by working with other DOJ components and government agencies, the private sector, academic institutions, and foreign counterparts, among others. In addition, DOJ's Criminal Division prosecutes violations of federal laws involving cyber intrusions and cyberattacks.

The FBI is the DOJ component with primary investigative authority for all computer network intrusions relating to threats to national security, including cases involving espionage, foreign counterintelligence, and information protected against unauthorized disclosure for reasons of national defense or foreign relations. As part of this work, the FBI exchanges information with other law enforcement entities through a network of fusion centers, according to FBI officials.[53] For example, FBI

[52]*National Defense Authorization Act for Fiscal Year 2020,* Pub. L. No. 116–92, § 3521(a), 133 Stat. 1198, 1988 (2019) (codified at 46 U.S.C. § 53202). The act directs the Secretary of Transportation, in consultation with the Secretary of Defense, to establish a fleet of active, commercially-viable cable vessels to meet national security requirements.

[53]Fusion centers are state-owned and -operated centers that serve as focal points in states and major urban areas for the receipt, analysis, gathering and sharing of threat-related information between state, local, tribal and territorial (SLTT), federal and private sector partners.

officials specifically highlighted that field offices in New Haven, Miami, Milwaukee, and Cleveland participate in local fusion centers and share intelligence on cybersecurity trends, threats, and vulnerabilities, among other information, with possible internet architecture security implications. In addition, FBI, through its field office private sector coordinators, shares homeland security and criminal-related information and intelligence that may directly or indirectly address internet architecture security.

Additionally, Coast Guard officials stated that the agency conducts waterborne patrols to deter and detect suspicious behavior in U.S. waters. These activities include preventing loitering around submarine cables. Coast Guard officials stated that they do not have any records of reported cases of such suspicious behaviors.

NIST Develops Security Standards

Commerce's NIST develops and deploys information security standards, guidance, best practices, and technology as part of its mission to improve the protection of federal government information systems. NIST also coordinates federal technical standards activities with private sector technical standards activities and develops standard interfaces, communications protocols, and data structures for computer and related telecommunications systems.[54]

Within this role, NIST collaborates with industry and academia to develop consensus cybersecurity standards that apply to internet architecture security. Specifically, NIST has coauthored numerous Internet Engineering Task Force (IETF) specifications that address internet architecture protection and supporting security technologies. Examples of these specifications include *Design Discussion of Route Leaks Solution Methods, Origin Validation Policy Considerations for Dropping Invalid Routes, and BGPsec Validation State Signaling.*

NIST also published security guidance and practice guide documents relating to the secure operation of BGP and DNS, including:

- Special Publication 800-81-2, a guide to assist organizations in understanding the secure deployment of DNS services in an enterprise;[55]

[54]See 15 U.S.C. § 272.

[55]NIST, *Secure Domain Name System (DNS) Deployment Guide,* Special Publication 800-81-2 (Gaithersburg, MD.: Sept. 2013).

- Special Publication 1800-14, a practice guide intended to improve the security and stability of the global internet by allowing networks to verify the validity of BGP routing information and strengthen the security and stability of the traffic flowing across the internet;[56]
- Special Publication 800-189, a guide intended to provide technical guidelines and recommendations for deploying protocols and technologies that improve the security of interdomain traffic exchange.[57]

FCC Regulates Portions of the U.S. Communication Network

The FCC impacts the security of networks that support the internet architecture as the regulator of interstate communications and communications between the United States and other countries.[58] FCC officials stated that the commission gives blanket authority for all telecommunications carriers to provide domestic interstate services or construct or operate domestic high-capacity transmission lines. The Commission also adjudicates applications filed by carriers to provide international telecommunications service. The Commission retains its authority to revoke any domestic or international authorization on a case-by-case basis to protect public interest. For example, in October 2021, it revoked one international entity's domestic authorization and revoked and terminated its international authority. The Commission's action was based in part on concerns raised by U.S. executive branch agencies about opportunities for foreign-government sponsored actors to disrupt and misroute U.S. internet traffic through BGP abuse. In January 2022, the Commission similarly revoked the authority of another international entity. FCC officials noted that no similar actions are being taken with respect to any U.S. owned and operated internet service provider.

In addition, FCC requires covered communications providers to report communications outages that meet certain thresholds related to the severity of the outage.[59] FCC staff from the Public Safety and Homeland Security Bureau stated that they review outage reports as well as other sources of private and public information to determine impacts on

[56]NIST, *Protecting the Integrity of the Internet Routing: Border Gateway Protocol (BGP) Route Origin Validation*, Special Publication 1800-14 (Gaithersburg, MD.: June 2019).

[57]NIST, *Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation*, Special Publication 800-189 (Gaithersburg, MD.: Dec. 2019).

[58]FCC's major statutory authority is the *Communications Act of 1934*, ch. 652, 48 Stat. 1064 (1934), as amended, including by the *Telecommunications Act of 1996*, Pub. L. No. 104-104, 110 Stat. 56 (1996); chapter 5 of title 47 U.S. Code.

[59]See, generally, 47 C.F.R. Part 4.

communications services and work with providers to understand the causes of outages. FCC staff noted that depending on the type and severity of an outage, the bureau may undertake a more in-depth investigation of particular outages, which can result in a report identifying the cause of the issue and any lessons learned. In one example of such a report, in October 2019, the FCC issued a public notice identifying cyber and physical security practices (such as making spare equipment geographically available and disabling unnecessary system features) that could have prevented or mitigated outages. Depending on the findings in these reports, the bureau may refer incidents to FCC's Enforcement Bureau for investigation into whether the Commission's rules were violated in connection with the outage.

Our June 2021 panelists noted that the federal government could help monitor market conditions and take actions to address any internet architecture security issues that could arise. Specifically, the panelists suggested that regulation could possibly be used to drive additional transparency (e.g. physical and cyber incident and outage data collection) surrounding the internet architecture market. Panel members also cautioned that there are potential challenges that could come with regulation. For example, increased data collection and sharing does come at a cost, and non-regulatory approaches like offering financial incentives might be appropriate. In addition, any technical security solutions identified in regulation may not be appropriate.

Relatedly, FCC staff has considered actions, such as those mentioned by panel members. For example, FCC staff researched an approach to monitoring for market failures in the cybersecurity market. In addition, FCC officials stated that as of October 2021, the commission is considering whether to extend outage reporting obligations to broadband services and the means to identify broadband outage trends. The officials noted that under existing rules, while the commission can infer internet outages through outages reported to other services, broadband internet service providers do not notify the commission directly of service outage. FCC officials also noted that the commission re-chartered CSRIC for a 2-year term that will end in June 2023. The FCC charged CSRIC with providing recommendations on topics including, among others, managing software and cloud services supply chain security for communications infrastructure.

Federal Programs Address Supply Chain-related National Security Concerns Affecting Internet Architecture

Federal agencies have internet architecture related supply chain security roles under the *Secure and Trusted Communications Networks Act of 2019*.[60] Specifically, FCC is to administer efforts to identify and to facilitate removing and replacing untrusted equipment or services that have been determined by law or executive branch national security organizations to pose an unacceptable risk to the national security of the United States, such as those used to deliver internet services. FCC officials stated the Commission completed the regulatory steps necessary to implement the program to accept applications to fund the replacement of equipment in October 2021. As of October 29, 2021, the program opened a website for companies to submit applications to FCC. The application filing window closed on January 28, 2022.

The 2019 act also directed NTIA to establish a program to share information regarding supply chain security risks with trusted communications providers and suppliers. In July 2020, NTIA announced the Communications Supply Chain Risk Information Partnership program with the intent to implement the program in a phased process. Subsequently, NTIA issued a plan for declassifying material, and stated that it is coordinating with DHS, ODNI, FBI, and the FCC.

Our June 2021 panelists noted that continued federal government involvement in addressing internet architecture supply chain risks would be beneficial, given the size and complexity of those supply chains.

DOD and NASA Operate Domain Name System Root Zone Servers

Although much of the internet's architecture is privately owned, certain federal agencies operate and secure hardware that routes internet traffic. Specifically, DOD and NASA components own and operate three of the 13 logical root zone servers that associate the IP address with the corresponding website as an initial step in the domain name system process.

- DISA and the Army Research Laboratory (ARL) operate the g.root and h.root servers, and have done so since 2005 and 1985, respectively. According to DISA officials, the g.root server operates within the DISA Information Systems Network, where it is subject to

[60]*Secure and Trusted Communications Networks Act of 2019*, Pub. L. No. 116-124, 134 Stat. 158 (2020), codified at 47 U.S.C. §§ 1601-1609.

the DOD Risk Management Framework, and the same DOD cybersecurity directives that apply to other DOD IT programs.[61]

- NASA's Ames Research Laboratory hosts the e.root server and has done so since 1987. The e.root server is subject to NASA IT security policies, the *Federal Information Security Modernization Act of 2014* and NIST guidance.[62] In 2019, DHS conducted a review of the e.root server to identify technical gaps and associated cybersecurity risks.[63] DHS's review pointed out the need for a cybersecurity governance structure to include documentation in support of an authority to operate. In August 2020, NASA completed a risk assessment for the server followed by a system security plan in October 2020 to document the authority to operate. The risk assessment identified threats and vulnerabilities based on physical and cybersecurity-related controls from NIST Special Publication 800-53 along with risk-reducing controls to mitigate them. It also included recommendations for improved monitoring of threats to the server. The related system security plan described specific actions implemented to align the e.root server's operations with NASA's systems security requirements.

Federal agencies also contribute to technical security activities of the root zone as a whole. For example, NTIA and NIST collaborated on a 2018 effort to update data related to encryption used in the root zone, which was necessary to maintain deployments of security technology in other systems in the DNS hierarchy. In addition, NASA officials stated that they, along with DISA and ARL, participate in ICANN's Root Server System Advisory Committee. The committee, comprised of server operators and representatives from internet governance organizations, meets monthly to discuss matters relating to the operation, administration, security, and integrity of the root server system.

[61]The DOD Risk Management Framework is intended to be consistent with NIST standards and guidelines developed to establish minimum cybersecurity requirements pursuant to the *Federal Information Security Modernization Act of 2014,* Pub. L. No. 113-283, 128 Stat. 3073 (2014).

[62]NIST, *Security and Privacy Controls for Federal Information Systems and Organizations*, SP 800-53, Rev. 5 (Gaithersburg, MD.: Dec. 2020).

[63]Pursuant to DHS, *Securing High Value Assets*, Binding Operational Directive (BOD) 16-01 (Washington, D.C.: Jun. 9, 2016), and its replacement, DHS, *Securing High Value Assets*, BOD 18-02 (Washington, D.C: May 7, 2018), DHS reviewed this agency-defined high value asset.

FCC Issues Licenses to Install and Operate Submarine Cable

The federal government issues, withholds, or revokes licenses to install cable landing stations or operate submarine cables in the United States. The FCC executes this role by taking steps to assess any national security and law enforcement concerns for companies with foreign ownership seeking to install and operate submarine cables. In its role of licensing cables, the Commission addresses several physical and cyber security topics.[64] In September 2021, FCC adopted a set of standardized national security and law enforcement questions that submarine cable license applicants with foreign ownership will be required to answer and submit directly to the executive branch agencies prior to or at the same time the applicants file their applications with the FCC.[65] FCC stated that these questions will facilitate the multi-agency executive branch review process established in Executive Order 13913.[66] These questions address physical and cyber security topics such as network controls access, communications content access, encryption use, and network peering connections. Further, FCC adopted rules to expand mandatory outage reporting to submarine cable services.[67] As of October 28, 2021, the FCC requires submarine cable operators to report to FCC specified unplanned service outages or degradation.[68]

Agency Comments

We requested comments on a draft of this report from the Department of Commerce, DOD, DHS, DOJ, Department of State, ODNI, NSF, the

[64]This authority for the FCC is delegated from the President of the United States in Executive Order 10530. The White House, *Providing for the performance of certain functions vested in or subject to the approval of the President,* Executive Order 10530 (Washington, D.C.: May 10, 1954).

[65]According to commission documents, these questions will also be applied to international telecommunications carriers seeking to provide service to the United States.

[66]The White House, *Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector*, Executive Order 13913 (Washington, D.C.: Apr. 4, 2020). This executive order formally established the committee to which the FCC can refer an application for advice and recommendations on national security and law enforcement concerns. The Attorney General chairs the committee and the Secretaries of Defense and Homeland Security are members. They are advised by several other federal officials, such as the Secretaries of State and Commerce and the Directors of National Intelligence and Office of Science and Technology Policy.

[67]*Improving Outage Reporting for Submarine Cables and Enhanced Submarine Cable Outage Dat*a, Report and Order, 31 FCC Rcd 7947; (2016), affirmed with modification, Order on Reconsideration, 34 FCC Rcd 13054 (2019).

[68]*Public Safety and Homeland Security Bureau Announces October 28, 2021 Compliance Date For Submarine Cable Outage Reporting Obligations*, Public Notice, 36 FCC Rcd 7589 (2021).

Office of Science and Technology Policy, FCC, and NASA. We received technical comments from Commerce, DHS, DOJ, ODNI, NSF, FCC, and NASA, which we incorporated as appropriate. DOD, the Department of State, and the Office of Science and Technology Policy stated that they had no comments on the draft report.

We are sending copies of this report to the appropriate congressional committees; the Secretaries of Commerce, Defense, Homeland Security, and State; the Attorney General of the United States; the Directors of National Intelligence and the National Science Foundation; the Office of Science and Technology Policy; the Chairwoman of the Federal Communications Commission; the Administrator of the National Aeronautics and Space Administration; and other interested parties. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (214) 777-5719, or hinchmand@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix II.

David B. Hinchman
Acting Director, Information Technology and Cybersecurity

Appendix I: Objectives, Scope, and Methodology

Our objectives were to (1) identify security risks related to the internet architecture and (2) determine the extent to which U.S. federal agencies have taken actions to address security risks to the internet architecture.

For the purposes of this report, “internet architecture” is defined in terms of select components that facilitate the transfer of data between connected high capacity networks. Specifically, these components are internet exchange points, high capacity cabling and information conduits, physical routing/switching infrastructure, border gateway protocol, and the domain name system. Our scope does not include any other components such as certificate authorities, web standards, or internet-based applications. Except for the domain name system (DNS) root servers operated by the federal government, we did not include any internet architecture components owned and operated by federal agencies in support of their use of the internet.

To identify the cyber and physical security risks to internet architecture components, we collected and analyzed publicly available reports from federal and nonfederal organizations. We identified applicable reports through various sources, including interviews with federal officials with relevant knowledge and internet searches using keywords like “risk,” “internet,” and “infrastructure.” In total, we analyzed nine federal and 16 nonfederal reports by reviewing each report and noting mentions of risk to in-scope internet architecture components. Examples of these reports include (1) a Department of Homeland Security 2017 risk assessment and (2) the Internet Corporation for Assigned Names and Numbers’ 2013 DNS Security and Stability Analysis Working Group report.[1] Based on the risks identified in the reports, we developed risk categories and assigned each mention of risk to a risk category. Additionally, we added risk categories and adjusted the language used to describe the risks and categories based on input from agency officials.

We also sought input on our risk categories from internet architecture subject matter experts. Specifically, we used the National Academies of Sciences, Engineering, and Medicine to identify internet architecture subject matter experts and we assembled two panels with willing experts during June 2021. The National Academies began its expert selection process by developing a core list of initial candidates. The candidates

[1]Department of Homeland Security, *Provide Domain Name Resolution Services and Provide Internet Routing, Access, and Connection Services Critical Functions Risk Assessment* (May 2017). The Internet Corporation for Assigned Names and Numbers, *DNS Security and Stability Analysis Working Group Final Report* (November 2013).

included current and former members of the National Academies' Computer Science and Telecommunications Board and the Forum on Cyber Resilience and members of government and inter-governmental organizations related to internet security such as the Internet Engineering Task Force. National Academies' staff contacted the candidates to (1) assess interest in contributing to GAO's planned focus groups and (2) gather further suggestions of potential candidates. National Academies' staff further contacted the suggested candidates.

As this process converged on a set of approximately 45 potential candidates, staff from the National Academies' and GAO staff examined the set of candidates and identified subject area gaps, such as physical layer security specialists and network operators, for additional canvassing and outreach. After the targeted outreach, the National Academies' and GAO staff compiled a final candidate set of approximately 50 names. The National Academies' staff conducted outreach to each of the names in the final candidate set to determine interest in participating in our expert panels.

Based on the candidates identified as being interested, GAO staff reviewed biographic information submitted by the candidates and determined which candidates to contact in order to arrange participation in one of two planned panel discussions. In June 2021, we assembled two panels totaling 17 of the experts.

- Joe Abley—Chief Technology Officer, Public Interest Registry (2019-2021)
- Fred Baker—Chair of the Internet Engineering Task Force (1996-2001), Chair of the Internet Society (2002-2008), Board Member of Internet Architecture Board (1996-2002), and Fellow at Cisco (1998-2016)
- Steven M. Bellovin—Percy K. and Vida L.W. Hudson Professor of Computer Science at Columbia University and affiliate faculty, Columbia Law School
- K.C. Claffy—Founder and Director of the Center for Applied Internet Data Analysis; and Adjunct Professor in the Computer Science and Engineering Department at University of California, San Diego
- Alissa Cooper—Vice President and Chief Technology Officer for Technology Policy and a Fellow at Cisco Systems, Chair of the Internet Engineering Task Force (2017-2021)

- Nick Feamster—Neubauer Professor of Computer Science and Data Science Institute Research Director at the University of Chicago
- Craig Labovitz—Deepfield Business Unit Chief Technology Officer in Nokia
- Martin Levy—Retired internet technologist and formerly with Cloudflare, Inc.
- Jason Livingood—Vice President of Technology Policy and Standards at Comcast and Board member of Internet Engineering Task Force Administration, LLC
- Milo Medin—Vice President of Wireless Services at Google, Inc.
- Michael R. Nelson—Senior Fellow, Technology and International Affairs at the Carnegie Endowment for International Peace
- Eric Rescorla—Internet Architecture Board member (2002-2008), and Internet Engineering Task Force Security Area Director (2017-2019)
- Jennifer Rexford—Professor and Chair of Computer Science at Princeton University
- Stefan Savage—Professor, Department of Computer Science and Engineering at the University of California, San Diego
- Bruce Schneier—Fellow and lecturer at Harvard Law School, and Chief of Security Architecture at Inrupt, Inc.
- Henning Schulzrinne—Levi Professor of Computer Science and Electrical Engineering at Columbia University, former Chief Technology Officer of the Federal Communications Commission (2011-2014, 2017), former technology fellow for Senator Ron Wyden (2019-2020)
- Bill Woodcock—Executive Director of Packet Clearing House

Panel discussions were held virtually and facilitated by a moderator from our Applied Research and Methods team. We did not attempt to gain consensus on any observation discussed, and no statement in our report is attributed to specific experts. As such, any reference to ‘panelists’ in this report means more than one (but not necessarily all 17) subject matter experts made a statement about an observation. During the panel sessions, we discussed cyber and physical risks identified in the previously analyzed reports and requested the experts to identify additional risks or concerns that were not identified. We also discussed federal government involvement in addressing the risks.

To determine the extent to which U.S. federal agencies have taken actions to address security risks to the internet architecture, we reviewed our prior work on internet governance and cybersecurity, as well as the *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021,* to identify existing cyber and physical security roles that have the potential to impact internet architecture components.[2] We determined that federal roles include, among others, (1) guiding critical infrastructure protection, (2) engaging in international partnership, (3) supporting technology research and development, (4) coordinating incident response, (5) investigating and prosecuting criminal activity, (6) developing security standards, and (7) regulating aspects of the U.S. communication network. In addition, through interviews and initial research, we identified federal roles for specific internet architecture components, such as operating three of the 13 domain name root servers. Based on these roles, we identified 10 federal agencies to include in our review: the Departments of Commerce, Defense, Homeland Security, Justice, and State; the Federal Communications Commission; the National Science Foundation; the National Aeronautics and Space Administration; the Office of the Director of National Intelligence; and the Office of Science and Technology Policy in the Executive Office of the President. We then collected and analyzed evidence of actions taken and conducted interviews with relevant officials from these agencies.

In addition, we discussed the roles of federal agencies in protecting internet architecture components, including agencies' involvement in risk activities and how well each agency had performed their role, with our subject matter expert panels. We also requested the experts discuss positive and negative impacts of the federal government in relation to their roles. Observations raised by the subject matter experts were then provided to pertinent officials with responsibility at the 10 selected federal agencies for comments.

[2]*William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021,* Pub. L. No. 116-283, § 9002(c), 134 Stat. 3388, 4770 (2021). Prior reports analyzed include: GAO, *Cybersecurity: Clarity of Leadership Urgently Needed to Fully Implement the National Strategy*, GAO-20-629 (Washington, D.C.: September 22, 2020); GAO, *Internet Management: Structured Evaluation Could Help Assess Proposed Transition of Key Domain Name and Other Technical Functions*, GAO-15-642 (Washington, D.C.: August 19, 2015); and GAO*, Communications Networks: Outcome-Based Measures Would Assist DHS in Assessing Effectiveness of Cybersecurity Efforts*, GAO-13-275 (Washington, D.C.: April 3, 2013).

We conducted this performance audit from October 2020 to March 2022 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 II: GAO Contact and Staff Acknowledgments

GAO Contacts

David B. Hinchman at (214) 777-5719, hinchmand@gao.gov

Staff Acknowledgments

In addition to the contact named above, Michael W. Gilmore (Assistant Director), Kenneth A. Johnson (Analyst-in-Charge), Jordan A. Adrian, Bradley W. Becker, Christopher Businsky, Saar Dagani, Franklin D. Jackson, Noah B. Levesque, Priscilla Smith, Andrew Stavisky, and Walter Vance made significant contributions to this report.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Phone

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

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

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

Connect with GAO

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

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

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

Congressional Relations

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

Public Affairs

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

Strategic Planning and External Liaison

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