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.

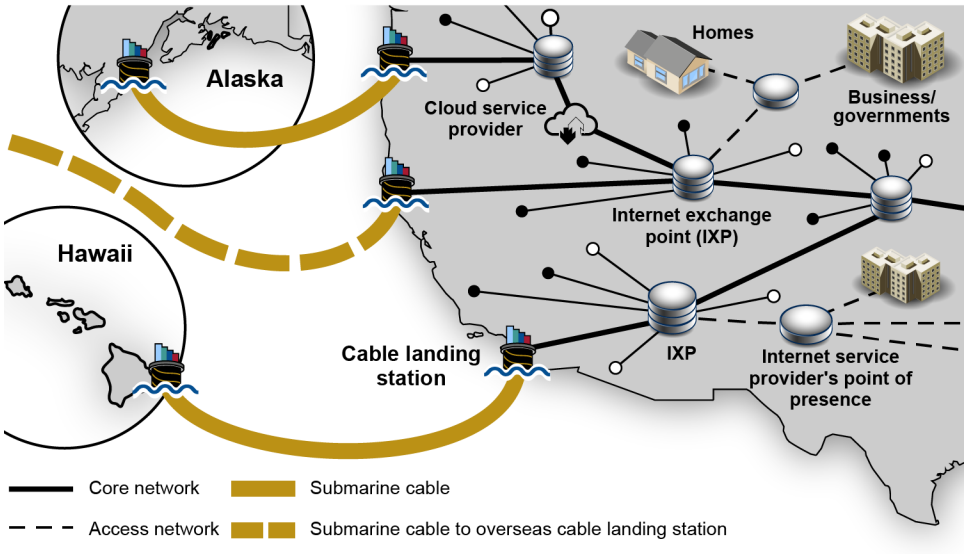
GAO collected and analyzed publicly available reports from federal and nonfederal organizations to identify risks to internet architecture components (internet exchange points, submarine cabling, the domain name system, and border gateway protocol, among others). GAO also reviewed federal law and policy 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