Federal Cybersecurity: Background and Issues for Congress

September 29, 2021

Congressional Research Service
https://crsreports.congress.gov
R46926

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R46926

September 29, 2021

Chris Jaikaran
Analyst in Cybersecurity Policy

Federal Cybersecurity: Background and Issues for Congress

Federal agencies are responsible for collecting, processing, storing, and disposing of a large amount of digital information related to individuals, businesses, and sensitive matters. Managing that data and the systems using the data in a secure way requires undertaking planning, implementing processes, and conducting programming on behalf of the agency—commonly referred to as *cybersecurity*.

Cybersecurity is a risk management process rather than an end-state. It involves continuous work to (1) identify and (2) protect against potential cybersecurity incidents; and to (3) detect; (4) respond to; and (5) recover from actual cybersecurity incidents. Agencies may choose to evaluate their information technology (IT) risks by understanding the threats they are susceptible to, the vulnerabilities they have, and the consequences a successful attack might have for their mission and their customers.

Federal agencies are subject to a variety of federal government-wide and agency-specific laws and guidance that address cybersecurity. Federal government-wide laws include the Federal Information Security Modernization Act of 2014 (FISMA), the Federal Information Technology Acquisition Reform Act of 2014 (FITARA), and the Privacy Act of 1974. Guidance documents include Office of Management and Budget (OMB) circulars and memoranda, and Department of Homeland Security (DHS) binding operational directives. Agencies are also subject to standards and guidance developed by the National Institute of Standards and Technology (NIST).

The FISMA delineates the federal roles and responsibilities for the cybersecurity of civilian agencies (commonly referred to as the *".gov" space*). Primary roles reside with the OMB, DHS, NIST, each agency, and each agency's inspector general (IG). In this model, OMB provides agencies strategic support, DHS provides agencies operational support, and each agency executes its own tactical-level cybersecurity actions.

Congress may choose to consider changes to federal cybersecurity management.

- **Positive Law Changes.** Agencies are subject to statutory requirements throughout the *U.S. Code*. Simplifying and unifying the statute, may provide opportunities for streamlined congressional oversight and clarified obligations for federal agencies.
- **Mandatory Reporting.** Policymakers may choose to consider the parameters pertaining to the structure and effect of a cyber incident reporting requirement: (1) who is required to report; (2) what is the threshold for reporting; (3) what information is reportable and when; (4) who receives the report; (5) how will the government process the report; and (6) how will the government further share the information?
- **Resource Levels.** Minimum spending levels (e.g., as a percentage of the agency's discretionary budget) may help to improve each agency's overall cybersecurity investment and provide opportunities to address historically under-resourced projects.
- **Shared Services.** The provisioning of cybersecurity services from each agency to a central agency may allow the federal government to better align and consolidate limited resources, such as trained and qualified cybersecurity workers.
- **New Cybersecurity Services.** Agencies may accelerate plans for moving toward next-generation cybersecurity services, such as endpoint detection and response (EDR) systems, highly adaptive cybersecurity services (HACS), and zero-trust architecture.

Contents

Tables

Contacts

Introduction

Federal agencies are responsible for collecting, processing, storing, and disposing of digital information. Managing that data and the systems using the data in a secure way requires undertaking planning, implementing processes, and conducting programming on behalf of the agency—commonly referred to as *cybersecurity*. Federal agencies regularly interact with nonfederal entities (such as federal contractors and critical infrastructure owners and operators) to gather information on cybersecurity issues and analyze ways to mitigate those issues, which would certainly have an impact on federal agencies, but could also have an impact on nonfederal entities, as well. Despite their efforts, there are instances in which the agencies fail and compromise information related to individuals, businesses, and sensitive matters.

This report begins with a discussion of cybersecurity principles and provides case examples of challenges to those principles. The report then provides an overview of policies related to federal cybersecurity by exploring and analyzing laws, agency guidance, and standards for cybersecurity, along with agency responsibilities for cybersecurity. This report concludes by examining options for Congress to address federal cybersecurity issues through updating statutes, requiring cyber incident reports, establishing cybersecurity funding levels, mandating the use of shared services, and/or requiring the adoption of modern cybersecurity tools.

Cybersecurity Principles

Cybersecurity is a risk management process rather than a static goal. It involves continual work to (1) identify and (2) protect against potential cybersecurity incidents; and to (3) detect; (4) respond to; and (5) recover from actual cybersecurity incidents. Agencies may choose to evaluate their information technology (IT) risks by understanding the threats they are susceptible to, the vulnerabilities they have, and the consequences of a successful attack for their mission and their customers.

The Office of Management and Budget (OMB) describes cybersecurity for federal agencies as follows:[1]

> 'Cybersecurity' means prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation.

Prior to purchasing a cybersecurity tool or implementing a new process, agencies must first understand what data and systems they possess, how those data and systems may be attacked, how likely those attacks are, and what challenges the agencies may face if their data and systems are impaired. This assessment helps to ensure that the agencies are taking a holistic approach to cybersecurity in a resource-limited environment. Agencies may consider threats, vulnerabilities, and consequences against the cybersecurity tenets of confidentiality, integrity, and availability (i.e., the C-I-A triad).

The concepts of *confidentiality*, *integrity*, and *availability* are defined in the *U.S. Code* as part of *information security*.[2] These terms apply to the data stored, processed, and transmitted by IT systems, but also to the IT systems themselves.

[1] Office of Management and Budget, *Managing Information as a Strategic Resource*, Circular No. A-130, Washington, DC, 2016, p. 28, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf.

[2] These definitions are at 44 U.S.C. §3552.

- *Confidentiality* refers to the attribute that data are known only to authorized parties and not made available or disclosed to unauthorized parties.
- *Integrity* refers to the attribute that data have not been altered or destroyed in an unauthorized manner.
- *Availability* refers to the attribute that data are available for access by an authorized party when they choose.

Two more terms were introduced after the acceptance of the C-I-A triad and occasionally supplement the definition of *information security*. *Authentication* is the ability to confirm that parties using a system and accessing data are who they claim to be and have legitimate access to that data and system. *Non-repudiation* refers to the ability of a sender of data to confirm delivery and the ability of a recipient to confirm the sender's identity, so that neither can deny having possessed the data.

Cybersecurity policy spans a range of fields, including education, workforce management, investment, entrepreneurship, and research and development. Software development, law enforcement, intelligence, incident response, and national defense may be involved in the response to cyberattacks.

Cybersecurity Challenges

Like the private sector, the U.S. government faces many threats in cyberspace. Three particular case studies highlight the threats federal agencies face from nation-state actors in cyberspace: the SolarWinds and Hafnium attacks in which adversaries compromised an IT product as a way of breaching the customers of those products; and the breach of Office of Personnel Management (OPM) databases. These attacks resulted in adversarial nations having access to sensitive government and citizen data and underscore the need for vigilance in pursuing cybersecurity.

SolarWinds

SolarWinds is a company that makes IT management products for business customers.[3] SolarWinds' products allow chief information officers (CIOs) to automate certain activities such as managing internet protocol (IP) addresses, monitoring devices on their networks, and deploying updates.

Russian[4] actors discovered a way to compromise SolarWinds' software development and update service for the Orion IT management platform (a SolarWinds suite of products). The actors then used access to the update channel to distribute malware. When run, the code executed the Sunburst malware in the SolarWinds IT management platform. Once executed, Sunburst would go dormant for a period of time (to avoid detection) before fetching additional instructions from its command-and-control (C2) server. The additional instructions allowed the adversaries to exfiltrate (steal) files, execute new commands, profile the system, and manipulate machines. The

[3] SolarWinds, https://www.solarwinds.com.

[4] "Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA)," January 5, 2021, at https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure.

adversaries sought to conceal their presence by manipulating files and disguising their activity as normal network traffic.

The versions of the platform that were vulnerable were released in spring 2020 through mid-December 2020. In December 2020, FireEye[5] (a cybersecurity company that first discovered the attack), SolarWinds,[6] and the Cybersecurity and Infrastructure Security Agency[7] (CISA) disclosed this attack. Shortly after, the government and industry issued tools to mitigate the exploit; CISA acknowledged that victims still needed to search for remnants of the adversary on their networks. (CISA directions to agencies in the wake of this attack are examples of guidance which is targeted to federal agencies, but were also shared with nonfederal entities for their consideration.)

The attack allowed the adversaries a foothold in their victims' networks. From there, they persisted in the network through the creation of additional credentials for other software platforms. Merely remediating the vulnerable versions of SolarWinds' products would have been insufficient to eradicate the unauthorized actors from a compromised network. Victims needed to actively threat-hunt for the adversaries on their networks and take further mitigating actions to expel the intruders.

SolarWinds stated that of their 300,000-plus customers, roughly 18,000 were susceptible to the attack.[8] As of February 17, 2021, nine federal agencies and approximately 100 private sector companies were known to have been compromised.[9]

Hafnium

Instead of compromising a platform to distribute malware (like in the SolarWinds attack), the Hafnium attack targeted IT infrastructure directly. Microsoft[10] and CISA[11] disclosed this attack in March 2021.

In the Hafnium attack, attackers exploited four zero-day vulnerabilities[12] against Microsoft Exchange Server (a mail server application) running on on-premises infrastructure (i.e., hardware deployed and maintained by the customer, as opposed to a cloud-service instance of Microsoft Exchange, such as Office 365). The Microsoft Exchange product provides email, calendar

[5] FireEye, "Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims with Sunburst Backdoor," blog post, December 13, 2020, at https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html.

[6] SolarWinds Corporation, "Current Report," Form8-K, December 14, 2020, at https://www.sec.gov/Archives/edgar/data/0001739942/000162828020017451/swi-20201214.htm.

[7] CISA, "Mitigate SolarWinds Orion Code Compromise," Emergency Directive 21-01, December 13, 2020, at https://cyber.dhs.gov/ed/21-01/#supplemental-guidance-v3.

[8] SolarWinds Corporation, "Current Report," Form 8-K, December 14, 2020, at https://www.sec.gov/Archives/edgar/data/0001739942/000162828020017451/swi-20201214.htm.

[9] Anne Neuberger, "Press Briefing by Press Secretary Jen Psaki and Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger, February 17, 2021," press briefing transcript, February 17, 2021, at https://www.whitehouse.gov/briefing-room/press-briefings/2021/02/17/press-briefing-by-press-secretary-jen-psaki-and-deputy-national-security-advisor-for-cyber-and-emerging-technology-anne-neuberger-february-17-2021/.

[10] Tom Burt, "New Nation-State Cyberattacks," blog post, March 2, 2021, at https://blogs.microsoft.com/on-the-issues/2021/03/02/new-nation-state-cyberattacks/.

[11] CISA, "Mitigate Microsoft Exchange On-Premises Product Vulnerabilities," Emergency Directive 21-02, at https://cyber.dhs.gov/ed/21-02/.

[12] A *zero-day vulnerability* (or 0-day) is a vulnerability to some hardware, firmware, or software which is unknown to users or the manufacturer at the time it is exploited. These vulnerabilities are not patched (or fixed by the manufacturer) and are difficult to protect against.

management, and contact management services. After exploiting these vulnerabilities, the attackers scripted commands to run on the compromised hardware, which allowed the attackers to steal data (e.g., email messages) and further embed into the victim's networks.[13]

Hafnium refers to the name the Microsoft Corporation has given to a set of actors that Microsoft says is operating on behalf of the People's Republic of China.[14] Microsoft, news reports, and this memorandum use the term "Hafnium" in reference to the most recent attack. However, the group Hafnium's activities are not limited to this attack. The U.S. government attributed these attacks to China on July 19, 2021.[15] An unknown number of on-premises Microsoft Exchange Server products were compromised by Hafnium.

Office of Personnel Management Breach

The Hafnium attack was not the first time the People's Republic of China compromised government data stores. In 2015, Chinese-government hackers accessed and exfiltrated personally identifiable information related to 21.5 million individuals, including 4.2 current and former federal employees, in two separate but related data breaches.[16] The compromised databases stored information related to background investigations and personnel records, and included such information as fingerprint data, Social Security Numbers, financial records, IT system credentials, and performance evaluations. According to the Federal Bureau of Investigation (FBI), the information taken in large data thefts allow China to identify targets for espionage campaigns and to help program artificial intelligence systems.[17]

In these attacks, it is unclear how hackers gained initial access to the Office of Personnel Management (OPM) networks. However, the OPM Inspector General (IG) had long reported cybersecurity deficiencies at the agency which went unaddressed for years.[18] Once hackers had access to OPMs systems, they entrenched into those systems, accessed the agency's Active Directory to gain root access, and spread malware through other systems.[19]

[13] Microsoft, "Hafnium Targeting Exchange Servers with 0-day Exploits," blog post, March 2, 2021, at https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/.

[14] Tom Burt, "New Nation-State Cyberattacks," blog post, March 2, 2021, at https://blogs.microsoft.com/on-the-issues/2021/03/02/new-nation-state-cyberattacks/.

[15] The White House, "The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China," statement, July 19, 2021, at https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/.

[16] U.S. Government Accountability Office, *Information Security: OPM Has Improved Controls, but Further Efforts are Needed*, GAO-17-614, August 2017, https://www.gao.gov/assets/gao-17-614.pdf.

[17] Christopher Wray, "The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States," Hudson Institute Video Event: *China's Attempt to Influence U.S. Institutions*, July 7, 2020, at https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states.

[18] U.S. Office of Personnel Management Office of the Inspector General, *Final Audit Report: Federal Information Security Modernization Act Audit*, Report Number 4A-CI-00-15-011, Washington, DC, November 10, 2015, https://www.opm.gov/our-inspector-general/publications/reports/2015/federal-information-security-modernization-act-audit-fy-2015-final-audit-report-4a-ci-00-15-011.pdf.

[19] Josh Fruhlinger, "The OPM Hack Explained: Bad Security Practices Meet China's Captain America," *CSO*, February 12, 2020, at https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html.

Significance of These Attacks

The U.S. government's inability to detect or prevent these attacks highlights the difficulty in curbing advanced, persistent threat (APTs) actors who are technically capable and motivated to conduct computer network operations (CNOs). Additionally, the large number of victims involved in or vulnerable to these attacks, and the scale of the attacks highlight the systemic nature of the cybersecurity risk faced by businesses and individuals. The nature of the data exposed or stolen through all these attacks also has the potential to disrupt government operations and increase threats to national security.

Policies

Congress has recognized the importance of protecting federal IT systems for decades. For example, the Computer Security Act of 1987 (P.L. 100-235) directed the Secretary of Commerce to work with the National Security Agency (NSA) to create standards and guidance for the protection of federal computer systems.[20] The Information Technology Management Reform Act of 1996 (P.L. 104-106, Title LI) required the National Institute of Standards and Technology (NIST) to promulgate compulsory standards necessary to improve the security and privacy of federal computer systems.[21] These compulsory standards are collected in the Federal Information Processing Standards (FIPS) publications.[22] Despite the age of some congressional and agency actions, those actions still have relevance in today's cybersecurity programs. For example, FIPS Publication 197 establishes the Advanced Encryption Standard (AES) as the cryptographic protocol federal agencies are to use when they have sensitive but unclassified information that requires protection.[23]

Most of the statutory requirements for secure digital communications were enacted during a period of static communications. That is, when users compose text-based messages on IT systems, transmit the encrypted messages to other users who, in turn, download them and read plaintext messages. The messages' composition, delivery, and receipt are distinct transactions. Traditional standard email is an example of this type of communication.

However, the internet has evolved over the past two decades. Static communications continue, but have been supplemented by dynamic communications. For example, written communications have transitioned to real-time, instant messaging. Real-time voice and video communications are also widely used. Both the federal government and the private sector have attempted to keep up with the evolving features of dynamic communications by adopting proprietary, commercial products (e.g., Microsoft's Skype for Business and Google's Workplace).[24]

---

[20] Citations for the Computer Security Act of 1987 were updated in 2003 with the passage of the Federal Information Security Management Act (P.L. 107-347) and the Federal Information Security Modernization Act of 2014 (P.L. 113-283). Both acts are referred to as FISMA and can be found in 44 U.S.C. Chapter 34, Subchapter II.

[21] 40 U.S.C. §11331.

[22] For a full list of current FIPS, see https://csrc.nist.gov/publications/fips.

[23] National Institute of Standards and Technology, *Announcing the Advanced Encryption Standard (AES)*, FIPS PUB 197, Washington, DC, November 26, 2001, at https://doi.org/10.6028/NIST.FIPS.197.

[24] For examples of communications tools used in the federal government, see National Security Agency, "Selecting and Safely Using Collaboration Services for Telework – UPDATE," cybersecurity information bulletin, June 2, 2020, at https://media.defense.gov/2020/Jun/03/2002310066/-1/-1/0/CSI-SELECTING-AND-USING-COLLABORATION-SERVICES-SECURELY-SHORT-20200602.PDF.

Popular exceptions to the adoption of dynamic communication methods are the continued reliance on email and commercial telephone services. Both email and telephone are widely available, interoperable among many providers, and provide a common means for government and citizens to communicate. However, while email and telephone services are ubiquitous, they are not secure. U.S. government officials have advocated for improved encryption of these communications platforms. Some examples of this advocacy include:

- In a 2019 interview with Michael Morell, the former Central Intelligence Agency (CIA) deputy director, Chris Krebs, the then-director of CISA, expressed a desire for inherently more secure commercial IT offerings.[25]
- In 2018, William Evanina, the then-nominee to be the director of the National Counterintelligence and Security Center (NCSC), advocated for unclassified government telephone calls to be encrypted given the threat of foreign intelligence service interception.[26]
- In 2017, CISA issued a directive to federal agencies to encrypt emails in transit and to implement policies to authenticate domain owners.[27]
- In 2010, Executive Order 13556 highlighted the inefficiency in securing and keeping private communications that are sensitive but unclassified (SBU) and created the Controlled Unclassified Communications program.[28]

These examples focus on specific forms of communication. However, agency cybersecurity policies rarely focus on specific communication platforms, instead opting for broad policies. Federal agencies are subject to a variety of federal government-wide and agency-specific laws and guidance that address cybersecurity. Brief discussions of major laws and guidance that are maximally applicable are provided below. Additional, more specific laws and guidance may apply under certain conditions but are not discussed here.

Federal Laws

Three federal statutes establish the main principles under which federal agencies secure their IT equipment and networks, and data. Primarily, these laws establish roles and responsibilities across the federal government rather than requiring specific security controls.

Federal Information Security Modernization Act of 2014 (FISMA)

The Federal Information Security Modernization Act of 2014 (FISMA)[29] establishes roles and responsibilities for federal agency information technology security. This version of FISMA is an update to the Federal Information Security Management Act of 2002 (Title III of the E-Government Act of 2002, P.L. 107-347). FISMA states that agency heads are ultimately

[25] Michael Morell, "Transcript: Chris Krebs talks with Michael Morell on 'Intelligence Matters,'" podcast, June 26, 2019, at https://www.cbsnews.com/news/transcript-chris-krebs-talks-with-michael-morell-on-intelligence-matters/.

[26] U.S. Congress, Senate Select Committee on Intelligence, *Nomination of William R. Evanina to be the Director of the National Counter Intelligence and Security Center*, 115th Cong., 2nd sess., May 15, 2018, S.Hrg. 115-396 (Washington: GPO, 2018), p. 16.

[27] CISA, *Enhance Email and Web Security*, Binding Operational Directive 18-01, October 16, 2017, at https://cyber.dhs.gov/bod/10-01/.

[28] Executive Office of the President, "Controlled Unclassified Information," 75 *Federal Register* 68675-68677, October 11, 2010.

[29] 44 U.S.C. §§3551-3559.

responsible for the security of their agency's IT, but may delegate those responsibilities to a senior agency official. In implementing their IT security programs, agencies must follow guidance issued by OMB and standards promulgated by NIST and each agency's inspector general (IG) must produce an annual evaluation of the agency's cybersecurity. The 2014 version of FISMA added a role for Department of Homeland Security (DHS), which is authorized to assist agencies in their IT security programs (this role is executed through CISA). IG evaluations of agency cybersecurity programs provide policymakers information on the performance of the agency. For example, in FY2020 the Department of Veterans Affairs (VA) IG examined the VA's compliance with FISMA.[30] That report made 26 recommendations to improve the agency's cybersecurity, 3 of which were new and 23 of which were carryovers from prior years. FISMA does not require agencies to implement specific cybersecurity strategies or use certain tools.

Other Laws

The Federal Information Technology Acquisition Reform Act of 2014 (FITARA)[31] expands the role of chief information officers (CIOs) in managing agency IT investments. Specifically, it requires CIOs to review and approve IT acquisitions for their agency and exercise governance and oversight over IT planning, programming, budgeting, and execution (PPBE) activities. While not primarily a cybersecurity law, it also requires CIOs to work with OMB to identify and improve the risk management of IT investments.

The Privacy Act of 1974[32] governs how agencies may collect and retain an individual's records and how they may or may not disclose that information to another party. The Privacy Act is agnostic to the medium upon which the information is stored, so has implications for how agencies store, process, and dispose of information held digitally in IT systems.

Of these laws, FISMA is the primary law governing how agencies address cybersecurity in their systems, data and networks, with FITARA and the Privacy Act providing amplifying directions to agencies. As Congress investigates agency cybersecurity performance, debates have coalesced around the idea of FISMA reform.[33] Options for such an update are discussed in the "Options for Congress" section.

Guidance

OMB, DHS, and the agencies develop and promulgate guidance for agency IT managers, each providing a different perspective. OMB provides broad, strategic directions, while DHS provides operational assistance to help agencies implement laws and guidance. Agencies produce policies and procedures to tactically execute a cybersecurity program against a backdrop of existing laws and guidance. (For further information see "Agency Roles.")

[30] Department of Veterans Affairs Office of Inspector General, *Federal Information Security Modernization Act Audit for Fiscal Year 2020*, Report #20-019727-104, Washington, DC, March 31, 2020, at https://www.va.gov/oig/pubs/VAOIG-20-01927-104.pdf.

[31] 40 U.S.C. §§11302, 11315, and 11319; and 44 U.S.C. §3601.

[32] 5 U.S.C. §552a.

[33] U.S. Senate Committee on Homeland Security and Government Affairs, *Federal Cybersecurity: America's Data Still at Risk*, staff report, August 2021, at https://www.hsgac.senate.gov/imo/media/doc/Federal%20Cybersecurity%20-%20America's%20Data%20Still%20at%20Risk%20(FINAL).pdf.

OMB Guidance

OMB issues memoranda and circulars, which agencies are obligated to follow for IT security.

OMB Circular A-108: ***Federal Agency Responsibilities for Review, Reporting, and Publication Under the Privacy Act.***[34] The Privacy Act of 1974[35] requires OMB to release additional guidance for agencies to comply with the Privacy Act. Circular A-108 establishes guidance for systems of records notices (SORNs),[36] reporting SORNs to OMB and Congress, implementation rules, exceptions, and how to account for the Privacy Act in other reporting.

OMB Circular A-123: ***Management's Responsibility for Enterprise Risk Management and Internal Control***[37] and ***Appendix A: Management of Reporting and Data Integrity Risk***[38] require agencies to identify and manage any risk to agency operations that may arise. Agencies may manage risk through the development and use of risk profiles and periodic reporting.

OMB Circular A-130: ***Management of Information as a Strategic Resource***[39] establishes general policy for the programming, planning, budgeting, and execution (PPBE) of IT resources (e.g., hardware, software, and personnel) that will use federal information. It includes appendixes for the protection of federal information resources and managing personally identifiable information.

OMB M-21-02: ***Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements***[40] provides guidance to agencies on implementing FISMA. It directs agencies to track certain metrics and use the Continuous Diagnostics and Mitigation (CDM)[41] dashboard provided by DHS, and includes reporting requirements.

DHS Guidance

DHS (acting through the CISA) issues Binding Operational Directives (BODs) for federal agencies to implement for the protection and security of federal information and IT systems. DHS is authorized to issue these compulsory directions under FISMA.[42] A selection of BODs that apply broadly over time is included below.

---

[34] Office of Management and Budget, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, Circular A-108, at https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A108/omb_circular_a_108_12_12_16.pdf.

[35] 5 U.S.C. §552a.

[36] A SORN is published by an agency when it develops or modifies a system (usually an IT system) that maintains a record about an individual.

[37] Office of Management and Budget, *OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control*, M-16-17, Washington, DC, July 15, 2016, at https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-17.pdf.

[38] Office of Management and Budget, *Appendix A to OMB Circular No. A-123, Management of Reporting and Data*, M-18-16, Washington, DC, June 6, 2018, at https://www.whitehouse.gov/wp-content/uploads/2018/06/M-18-16.pdf.

[39] Office of Management and Budget, *Managing Information as a Strategic Resource*, Circular No. A-130, Washington, DC, July 28, 2016, at https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf.

[40] Office of Management and Budget, *Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements*, M-21-02, Washington, DC, November 9, 2020, at https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-02.pdf.

[41] Cybersecurity and Infrastructure Security Agency, Continuous Diagnostics and Mitigation (CDM), website, at https://www.cisa.gov/cdm.

[42] 44 U.S.C. §3553.

BOD 18-02: ***Securing High Value Assets***[43] is a DHS order that requires agencies to identify and report their high-value IT assets to DHS, allowing DHS to assess the security of those assets, and mitigate any vulnerabilities that DHS finds within 30 days.

BOD 19-02: ***Vulnerability Remediation Requirements for Internet-Accessible Systems***[44] is a DHS order that requires agencies to review and mitigate DHS-found vulnerabilities on internet-accessible IT systems within 30 days of notification.

BOD 20-01: ***Develop and Publish a Vulnerability Disclosure Policy***[45] is a DHS order that requires agencies to create and publish policies on how the public can identify vulnerabilities in federal IT systems and alert the agency of the potential risk.

As FISMA establishes roles and responsibilities for cybersecurity, these documents further assist those incumbent to those roles in achieving their responsibilities. Some guidance documents seek to provide agencies with specific actions to improve cybersecurity programs (e.g., BOD 20-01). Some documents provide broad activities agency should engage in, and in doing so should see improved cybersecurity effectiveness (e.g., OMB Circular A-130). However, these guidance documents are not categorically enforced. The Government Accountability Office (GAO) found that agencies continue to have weak cybersecurity because of ineffective programs.[46] Policymakers may choose to review the number, nature, and effectiveness of guidance documents. In doing so, harmonizing, reducing, or amplifying guidance documents may provide agencies with clearer objectives for their cybersecurity programs. Policymakers may also choose to alter how these policy documents are enforced. Currently, agencies may petition the OMB Director (or Secretary of Homeland Security for BODs) for a waiver on the policy. Additionally, agencies may poorly implement the policy with little consequences.

Standards

Federal agencies are subject to standards and guidance developed by NIST.[47] NIST standards for federal agencies may be published as a Federal Information Processing Standard (FIPS), NIST Interagency Report (NISTIR), or Special Report (SP). A selection of widely applicable NIST documents is provided below.

FIPS Publication 199: ***Standards for Security Categorization of Federal Information and Information Systems***[48] is a standard federal agencies must follow to assess their information and IT systems, so that appropriate security measures may be applied.

---

[43] Cybersecurity and Infrastructure Security Agency, *Securing High Value Assets*, Binding Operational Directive 18-02, May 7, 2018, at https://cyber.dhs.gov/bod/18-02/.

[44] Cybersecurity and Infrastructure Security Agency, *Vulnerability Remediation Requirements for Internet-Accessible Systems*, Binding Operational Directive 19-02, April 29, 2019, at https://cyber.dhs.gov/bod/19-02/.

[45] Cybersecurity and Infrastructure Security Agency, *Develop and Publish a Vulnerability Disclosure Policy*, Binding Operational Directive 20-01, September 2, 2020, at https://cyber.dhs.gov/bod/20-01/.

[46] U.S. Government Accountability Office, *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges*, GAO-21-228, March 2021, https://www.gao.gov/assets/gao-21-288.pdf.

[47] 15 U.S.C. §278g–3 and 40 U.S.C. §11331.

[48] National Institute of Standards and Technology, *Standards for Security Categorization of Federal Information and Information Systems*, FIPS PUB 199, Gaithersburg, MD, February 2004, at https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf.

FIPS Publication 200: ***Minimum Security Requirement for Federal Information and Information Systems***[49] is a complementary standard to FIPS Publication 199. It provides the 17 minimum security requirements agencies must follow for IT systems.

NISTIR 8170: ***Approaches for Federal Agencies to Use the Cybersecurity Framework***[50] provides examples that agencies may follow to use the *Framework for Improving Critical Infrastructure Cybersecurity*[51] in accordance with Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*.[52]

SP 800-37: ***Risk Management Framework for Information Systems and Organizations***[53] provides a risk management framework for agencies to follow to determine a security categorization for an IT system. Security categorizations are based on the information security principles of confidentiality, availability, and integrity[54] and are recorded as *low*, *moderate*, or *high*. The security categorizations inform which security measures an IT system must use.

SP 800-53: ***Security and Privacy Controls for Information Systems and Organizations***[55] provides agencies with a catalog of security and privacy requirements agencies must implement for their IT systems.

Stakeholders frequently deride FISMA as being an ineffective framework for managing cybersecurity.[56] However, many of their arguments are not about the statute itself. Rather, complaints are generally about an agency's implementation of FISMA or implementing guidance. Policymakers may also seek to change how the guidance and strategy documents are issued. Many times these documents are issued or altered following a cybersecurity incident and the changes the incident brings about become permanent. However, this process is reactionary and sometimes burdens agencies with requirements that resolve one issue while being blind to

[49] National Institute of Standards and Technology, *Minimum Security Requirements for Federal Information and Information Systems*, FIPS PUB 200, Gaithersburg, MD, March 2006, at https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf.

[50] Matt Barrett et al., *Approaches for Federal Agencies to Use the Cybersecurity Framework*, National Institute of Standards and Technology, NISTIR 8170, March 2020, at https://doi.org/10.6028/NIST.IR.8170.

[51] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, April 16, 2018, at https://doi.org/10.6028/NIST.CSWP.04162018.

[52] Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," 82 *Federal Register* 22391-22397, May 16, 2017.

[53] National Institute of Standards and Technology, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, SP 800-37, December 2018, at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf.

[54] The terms *information security*, *confidentiality*, *availability*, and *integrity* are defined in 44 U.S.C. §3552 as follows:
"The term 'information security' means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide-
(A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;
(B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
(C) availability, which means ensuring timely and reliable access to and use of information."

[55] National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, SP 800-53, September 2020, at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

[56] For examples, see Paul Rosenzweig, "Why Federal IT Will Never Be Secure," *Lawfare*, February 21, 2017, at https://www.lawfareblog.com/why-federal-it-will-never-be-secure; and Brian Robinson, "FISMA Compliance Falls Short of Adequate Security," *FCW*, 2011, at https://fcw.com/microsites/2011/securing-government-systems/fisma-compliance-inadequate-security-of-government-systems.aspx?m=1.

another. Periodic and comprehensive reviews of guidance documents may ensure that federal cybersecurity programs remain current and effective against evolving threats. However, changes to guidance carry resource burdens which agencies may be unable to bear.

Agency Roles

The Federal Information Security Modernization Act of 2014 (FISMA; P.L. 113-283)[57] delineates the federal roles and responsibilities for the cybersecurity of civilian agencies (commonly referred to as the *".gov" space*). Primary roles are assigned to OMB, DHS/CISA, NIST, each federal agency, and each agency's IG. In this model, OMB provides agencies strategic support, DHS provides agencies operational support, and each agency executes its own tactical-level cybersecurity actions.

The Office of Management and Budget, exercising its oversight of agency budgets, is responsible for overseeing agency adoption of cybersecurity practices and guiding agencies to a cybersecurity posture commensurate to their risk. Through its budgetary authority, OMB enforces the adoption of cybersecurity practices by directing the expenditure of funds for this purpose. OMB may also install new senior officials to oversee mismanaged cybersecurity programs, but CRS was unable to find an instance of OMB exercising this authority.[58] OMB also annually reports to Congress on overall agency cybersecurity performance and provides summaries of agency evaluations.[59]

The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency oversees agency adoption of cybersecurity programs, provides tools to protect agency networks, and coordinates government-wide efforts on federal cybersecurity. DHS also mandates agencies take certain cybersecurity actions on their networks to mitigate immediate risks or implement processes to improve their overall cybersecurity.[60]

Agency heads are ultimately responsible for ensuring that risks are effectively managed in their own organization, with cybersecurity being one such risk (financial and operational risk are among the others). In accordance with FISMA, agency heads shall delegate the responsibility for cybersecurity to a senior official, frequently a chief information security officer.[61]

The National Institute of Standards and Technology develops standards (e.g., the Federal Information Processing Standards) and guidance (e.g., Special Publications) to inform agencies of security practices to adopt.[62] Agencies are compelled to adopt these standards;[63] however, OMB, not NIST, is responsible for ensuring agency adoption.[64] NIST's standards and guidance are also

[57] 44 U.S.C. Chapter 35, Subchapter II.

[58] 40 U.S.C. §11303.

[59] For an example, see Office of Management and Budget, "Federal Information Security Modernization Act 2014: Annual Report to Congress," *FISMA FY 2019 Annual Report to Congress*, May 2020, at https://www.whitehouse.gov/wp-content/uploads/2020/05/2019-FISMARMAs.pdf.

[60] For more information on DHS's cybersecurity responsibilities, see CRS In Focus IF10683, *DHS's Cybersecurity Mission—An Overview*, by Chris Jaikaran.

[61] 44 U.S.C. §3554, (a)(3)(A).

[62] NIST, "FIPS Publications," website, October 16, 2015, at http://csrc.nist.gov/publications/PubsFIPS.html; and NIST, "Special Publications," website, April 8, 2016, at http://csrc.nist.gov/publications/PubsSPs.html.

[63] 15 U.S.C. §278g–3.

[64] 44 U.S.C. §3553.

applicable to agency contractors and any other organization that operates a system or processes data on behalf of the federal government.

Inspectors General annually evaluate their agency's cybersecurity programs and provide recommendations on improving their agency's cybersecurity posture. IGs may lack the capability or capacity to perform evaluations of agency IT security, so may opt to contract out this work. Commonly, IGs piggyback on contracts that agency chief financial officers solicit for independent evaluation of agency financial management and have those vendors perform the IT security audit under the auspices of the IG.

The **Comptroller General** may also periodically evaluate and report to Congress on agency information security policies and practices.[65]

The **National Cyber Director** (NCD) was recently created (P.L. 116-283, §1752)[66] to provide a single official with the responsibility of overseeing a national cybersecurity strategy and advising the President. In establishing the NCD, Congress implemented a recommendation from the Cyberspace Solarium Commission.[67] While this position predominately focuses on national cybersecurity issues, it does carry the responsibility to work with other agency heads to streamline federal policy and guidelines related to FISMA. Additionally, the NCD is responsible for developing a National Cyber Strategy. Nothing prohibits this strategy from including provisions related to federal agency cybersecurity. The NCD also carries responsibilities for reviewing agency budget proposals and assessing agency implementation of the strategy and other cybersecurity policies.

Options for Congress

Congress may choose to consider changes to federal cybersecurity management. In doing so, it may assess and consider revisions to (1) positive laws; (2) requirements for mandatory reporting; (3) resource levels; (4) the use of shared services; and (5) the use of new cybersecurity services.

Positive Law Updates

Federal agencies are subject to many cybersecurity requirements in the *U.S. Code*. The majority of those requirements exist in Title 44 of the *U.S. Code*, Chapter 35, Subchapter II, where FISMA is codified. Additional requirements exist in Title 6, Chapter 6 and in Title 40, Subtitle III.[68] Congress may choose to revisit the codification of federal cybersecurity requirements across the *U.S. Code* to simplify and unify the statute. In doing so, Congress may provide opportunities for streamlined oversight and clarified obligations for federal agencies.

Additionally, Congress may choose to investigate existing responsibilities, their distribution, and how roles work with each other. There are many federal officials responsible for government-wide cybersecurity. Congress created the National Cyber Director less than a year ago. The E-

[65] For examples, see U.S. Government Accountability Office, *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges*, GAO-21-288, March 24, 2021, https://www.gao.gov/products/gao-21-288; and U.S. Government Accountability Office, *Weapon Systems Cybersecurity: Guidance Would Help DOD Programs Better Communicate Requirement to Contractors*, GAO-21-179, March 4, 2021, https://www.gao.gov/products/gao-21-179.

[66] 6 U.S.C. §1500.

[67] For further information on the Cyberspace Solarium Commission, see CRS In Focus IF11469, *The Cyberspace Solarium Commission: Illuminating Options for Layered Deterrence*, by Chris Jaikaran, and https://www.solarium.gov.

[68] Other agencies have additional requirements, such as those for NIST in 15 U.S.C. §278g–3 and VA in 38 U.S.C. §§5721-5728.

Government Act created the Director of the Office of E-Government, and that individual nominally serves as the Federal Chief Information Office; however, the Federal CIO position does not exist in law. Additionally, the role of the Federal Chief Information Security Officer (CISO) has been filled in the past few administrations at the discretion of the President, but it too does not exist in statute. The 115th Congress created the Cybersecurity and Infrastructure Security Agency (CISA) with responsibilities for managing risks to federal cybersecurity and created a Director to lead the agency. In instances where Congress created positions, legislation generally required those positions to coordinate with other officials, but was silent on the nature of that coordination. Congress may choose to authorize the Federal CISO in statute and authorize the Federal CIO position as the Director of the Office of E-Government. In doing so, Congress may also choose to delineate the specific responsibilities of the NCD, Federal CIO, Federal CISO, and the Director of CISA and describe how, and under what circumstances, those positions shall coordinate.

Mandatory Reporting

The 117th Congress has debated requiring nonfederal entities to report to a federal agency when the entity experiences a cyberattack. Because of the rising frequency and severity of ransomware attacks,[69] some see the debate on reporting as an evolution of the debates concerning data breach notification requirements during the 115th and 116th Congresses.[70] Independently, others see cyber incident reporting as a necessary tool for policymakers and authorities to better understand cyber threats in their own right.[71]

In examining threats to federal information technology and data, officials seek to collect information not just from federal agencies, but also from nonfederal entities which may store or process government information, or operate federal systems on behalf of the government. Irrespective of individual contracts, Executive Order 14028, *Improving the Nation's Cybersecurity*, requires entities providing information and communications technology to the federal government to report to CISA when they discover a cyber incident on a product or service used by the government.[72]

Generally, requirements for cyber incident reporting are not new. Many regulated entities are required to report to one or more federal agencies when they experience a cyber incident and provide information on the nature of that incident. By collecting this information, the government is seeking to both improve the protection of its technology (and the data in its possession) and understand broader risks facing the nation. **Table 1** provides a brief review of selected reporting requirements.

[69] For an example, see CRS Insight IN11667, *Colonial Pipeline: The DarkSide Strikes*, by Paul W. Parfomak and Chris Jaikaran.

[70] Brad D. Williams, "Senators Introduce Bill Requiring Notification of Cyber Incidents within 24 Hours," *Breaking Defense*, July 21, 2021, at https://breakingdefense.com/2021/07/senators-introduce-bill-requiring-notification-of-cyber-incidents-within-24-hours/.

[71] Cyberspace Solarium Commission, "Cyberspace Solarium Commission," final report, March 2020, at https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view.

[72] Executive Office of the President, "Improving the Nation's Cybersecurity," 86 *Federal Register* 26633-26647, May 12, 2021.

Table 1. Selected Cyber Incident Reporting Requirements

Sector	Reporting Entity	Receiving Entity	Requirement	Authority
Federal Government	Federal Agencies	OMB, CISA, Congressional Committees	Report significant cyber incidents within OMB-prescribed time frames.	44 U.S.C. §3554 M-21-02
Communications	Undersea Cable Operators	FCC	Report outages related to submarine cables.	47 C.F.R. Part 4
Defense Industrial Base	Defense Contractors	DOD	Analyze and report cyber incidents affecting covered defense information.	48 C.F.R. §§204, 212, 217, 252
Energy	Electricity Providers	FERC	Report cyber incidents if they have compromised or disrupted one or more tasks related to the reliability of energy distribution.	7 C.F.R. §1730 CIP-008-05
Financial Services	Financial Institutions	Financial Regulators	Report to regulators instances of unauthorized access to nonpublic customer information.	12 C.F.R. Part 30 12 C.F.R. Parts 208 and 225 12 C.F.R. Part 364 12 C.F.R. Parts 568 and 570
Health Care	Covered Health Care Institutions	HHS	Report losses of protected health information.	45 C.F.R. §160 and Subparts A and E of Part 164
Nuclear	Nuclear Licensees	NRC	Report cyber incidents that affect safety, security, emergency preparedness, or support systems of a nuclear site within one hour of discovery.	10 C.F.R. §73.77
Transportation	Pipeline Operators	TSA and CISA	Report actual or suspected cyberattacks that could impact industrial control systems, measurement or telemetry systems, or enterprise IT.	49 C.F.R. §114

Source: CRS analysis.

Notes: Office of Management and Budget (OMB), Memorandum on the Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements (M-21-02). The following abbreviations appear in the table: Cybersecurity and Infrastructure Security Agency (CISA); Federal Communications Commission (FCC); Department of Defense (DOD); Federal Energy Regulatory Commission (FERC); Critical Infrastructure Protection Reliability Standard (CIP); Department of Health and Human Services (HHS); Nuclear Regulatory Commission (NRC); Transportation Security Agency (TSA); Information Technology (IT); Department of Education (ED); *U.S. Code* (U.S.C.); and *Code of Federal Regulations* (C.F.R.).
Depending on the financial institution, the financial regulator for cyber incident reporting may include the Federal Reserve System Board of Governors, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, the Consumer Financial Protection Bureau, and state regulatory agencies.

Framework for Cyber Incident Reporting

As Congress continues to debate the need for cyber incident reporting, policymakers may choose to consider the following six parameters pertaining to the structure and effect of a cyber incident reporting requirement:

1. who is required to report;
2. what is the threshold for a reportable incident;
3. what information is reported and when;
4. who receives the report;
5. how will the government process the report; and
6. will the information be shared, and how?

This framework may be applied to reports from one federal agency to another, for federal contractors providing information to an agency, or broadly in instances where nonfederal entities are required to share cyber incident information with the government.

Who Is Required to Report

A primary concern in establishing a requirement is delineating to whom it applies. In reviewing federal cybersecurity rules, most are not applicable to all parties at all times. Instead, federal cybersecurity rules are narrowly applicable to a defined set of stakeholders.[73] Most existing reporting requirements for cyber incidents follow a dual-criteria constraint: the requirement only applies to a *covered entity* and only for *covered information.* For example, if a hospital experiences a data breach and exposes the health information of its patients, then that is an example of a covered entity losing the confidentiality of covered information, and the hospital must report that incident to authorities. However, if a law enforcement agency has the same information and they lose it, then that event is not reportable—even though the data may be covered, the entity holding the information is not. Congress may choose to continue with the dual-criteria constraint, requiring cyber incident reporting for a defined set of entities and a defined category of data. Congress may choose to define the sets of entities or data narrowly or broadly. This could include requiring any entity to report a cyber incident involving specific data in its custody. Regulated entities would likely request clarity on whether or not reporting requirements apply to them, and under what circumstances the requirement applies (e.g., for all attacks, or only attacks affecting certain systems or data).

What Is the Threshold for a Reportable Incident

Depending on its size, an entity may face hundreds, thousands, or millions of adverse cyber events daily. These events exist on a spectrum from mild to severe. Some of these events are handled with automated tools (e.g., filtering spam messages or malicious websites). Other events evade automated tools and result in an event that administrators manage (e.g., unauthorized access to a resource that is detected and mitigated). Other incidents result in a malicious actor gaining access to a sensitive data store or system and/or gaining further access into a system, resulting in a persistent compromise (e.g., the SolarWinds attack). Congress may choose to prescribe the threshold for a reportable event or direct an agency to do so. For example, under the

[73] For further information on data protection laws, see CRS Report R45631, *Data Protection Law: An Overview*, by Stephen P. Mulligan and Chris D. Linebaugh. Certain rules like the Children's Online Privacy Protection Rule (COPPA) are an exception—the rule is applicable to a defined set of data (i.e., data about minors) as opposed to all data.

Federal Energy Regulatory Commission (FERC) requirement for incident reporting, only events that have the potential to compromise the reliability of power systems warrant reporting under the regulation. Clarity for entities on the types of incidents that warrant reporting, and what incidents warrant enhanced or multiple-party reporting, could help reduce the burden on reporting entities and ensure the government receives consistently reported information.

What Information Is Reported and When

Once an entity detects a possible cyber incident (e.g., receives a notification of a ransomware attack or observes a suspicious administrative credential on their network), or is informed by an outside party (e.g., a law enforcement agency) that the entity may have suffered an attack, then the entity can begin an investigation into the incident. The information the entity must provide as part of its cyber incident reporting can serve various purposes for the government. For instance, simple information about the event (e.g., the nature of the event; the time, date, and duration; and types of systems or data compromised) may provide indicators of the frequency, scope, and scale of certain attacks in aggregate across many potential victims. However, additional information (e.g., vulnerabilities exploited by the malicious actors, method of detection, response actions, and the security status of the system prior to the incident) may provide federal agencies with additional information about the threat actors; their techniques, tactics, and procedures (TTPs); and opportunities to inhibit future attacks. Congress may choose to require a single report when sufficient information is available. Alternatively, Congress may choose to require entities to file periodic and/or regular reports as incidents unfold. For example, federal agencies must provide notice within 7 days to Congress when the agency becomes aware of a major attack, and then supplement that information within 30 days with amplifying information (e.g., an estimate of the number of individuals affected).[74]

Who Receives Reports

Entities need to know which federal agency or agencies they must notify when they become the victim of a cyber incident. The requirement creates a relationship between that entity and the agency to which it reports. Entities may be hesitant to submit their data to law enforcement agencies for fear that they may become the subject of an investigation; to regulators for fear that they may become the target of regulatory action; and to agencies without information protection rules in place for fear that the entity's information may be releasable under a Freedom of Information Act (FOIA) request or as part of court proceedings. Alternatively, entities may be more comfortable submitting their data to a federal agency with which they have a history of engagement and with which the entity regularly shares information.

It has long been the policy of the U.S. government that entities that experience cyberattacks are victims and that the government will not seek to further punish victims by seeking punitive actions against the company (e.g., investigating the company for possible criminal liability)—a policy that Congress may choose to examine, reinforce, or alter.

How Will the Government Process the Report

Once cyber event information is in the possession of the government, what will the government do with it? The amount, type, and timeliness of the reported data can provide valuable insights into the evolving nature of the nation's cybersecurity risk. Conversely, the reported data may

[74] Office of Management and Budget, "Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements," M-21-02, November 9, 2020, at https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-02.pdf.

contain sensitive information, making it a potential target for adversaries. Government agencies will simultaneously seek to process the data while also protecting it. There may be a desire to classify the data when in the possession of the government to increase its security, as national security systems are generally not connected to the public internet and allow for a securer environment in which the government may combine various sources of information to conduct analysis. At the same time, working with classified material is a challenge for nonfederal entities. The media used by entities to report would likely be unclassified. Additionally, classifying the data makes accessing it more difficult for both federal and nonfederal recipients, as they must have the requisite national security clearance to read the information.

In processing the data, the government may seek to identify new threat vectors; commonly exploited vulnerabilities; the techniques, tactics, and procedures (TTPs) of adversaries; and successful risk-mitigation strategies, among other data elements. Regardless of which agency receives the information, agencies may be required to share cyber incident reports with a central agency (or agencies) for aggregation and analysis. This step of the analysis could help ensure that policymakers have updated data on evolving risks to inform the legislative debate. Additionally, centralized aggregation and analysis would allow the central agency (or agencies) the opportunity to identify trends and gain insights into the nation's cybersecurity risk, which the agency (or agencies) may then use to develop and distribute cybersecurity risk-mitigation products.

Additionally, how the government would retain the information for future use and dispose of the information when no longer needed may need to be determined. The agency that principally collects and processes the data will likely complete assessments related to the privacy and records management implications of the system and determine how the data shall be treated. Congress may choose to address these concerns in legislation.

Will the Information Be Shared, and How

An agency could potentially share information gleaned from a cyber incident report, or the entire report. Whether or how an agency does so would be a matter of policy that could be mandated by Congress. The data held by agencies has value beyond the federal government. Nongovernmental entities can use data on cyber incident trends to target investments in cybersecurity risk-mitigation technologies. Insurance companies can use information on cyber incidents to improve their actuarial data and set rates. State and local governments can use cyber incident data to engage in their own policymaking and legislative debates. Depending on the sensitivity of the data in the cyber incident report, the agency may have obligations under the Privacy Act of 1974.[75] An agency may be required to anonymize data before releasing information. Additionally, an agency may also be tasked with regular (e.g., monthly, quarterly, or annually) reports on the state of cyber risk based on cyber incident reporting.

Assess Funding Levels

The Consolidated Appropriations Act, 2017 (P.L. 115-31) requires the President to include an analysis of agency cybersecurity funding in the President's annual budget submission to Congress.[76] For FY2019-2022, OMB included in the annual budget request an Analytical Perspective on "Cybersecurity Funding," which provided agency-reported expenditures and planned expenditures for cybersecurity. Using that data, combined with OMB's reporting of

[75] 5 U.S.C. §552a.

[76] 31 U.S.C. §1105.

major agency base discretionary funding, one can analyze agency budgets to see how much money an agency spends on cybersecurity.

The base discretionary funding provided through the regular annual appropriations process is not the total budget an agency may have to spend in a given fiscal year. Mandatory spending and emergency supplemental appropriations can increase an agency's overall budget. Base discretionary funding is used for cross-agency comparison because agencies may not receive mandatory funding for their operations, and emergency funding generally responds to specific crises (rather than reflects policy priorities in cybersecurity). **Tables 2-7** present cabinet department and major agency base discretionary funding and cybersecurity funding—both in dollars and as a percentage of base funding—for each fiscal year from FY2017 through FY2022. This is based on the information provided in the Analytical Perspectives budget documents from FY2019 through FY2022, using the most complete data available for each year. **Table 8** summarizes each department's and major agency's cybersecurity funding as a percentage of its base discretionary funding for each fiscal year over the six-year period, FY2017 through FY2022.

Table 2. FY2017 Major Agency Cybersecurity Funding

Cybersecurity Funding Relative to Base Net Discretionary Budget Authority, in millions of nominal dollars

Agency	Base Discretionary (Estimate)	Cybersecurity Funding (Actual)	Cybersecurity Funding as a % of Base Discretionary
Agriculture	$22,700	$115	0.50%
Commerce	$9,300	$274	2.94%
Defense	$523,200	$7,224	1.38%
Education	$66,900	$74	0.11%
Energy	$30,200	$371	1.23%
HHS	$87,100	$320	0.37%
Homeland Security	$42,400	$1,614	3.81%
HUD	$48,000	$15	0.03%
Interior	$13,500	$84	0.62%
Justice	$28,400	$735	2.59%
Labor	$12,000	$83	0.70%
State	$38,700	$254	0.66%
Transportation	$19,300	$185	0.96%
Treasury	$12,700	$458	3.61%
Veterans Affairs	$74,400	$386	0.52%
EPA	$8,200	$25	0.31%
NASA	$19,700	$148	0.75%
NSF	$7,500	$183	2.44%
SBA	$800	$20	2.44%

Source: Office of Management and Budget, *Efficient, Effective, Accountable: An American Budget*, Fiscal Year 2019, Washington, DC, February 12, 2018, p. 144, https://www.govinfo.gov/content/pkg/BUDGET-2019-BUD/pdf/BUDGET-2019-BUD.pdf. Office of Management and Budget, *Analytic Perspectives*, Fiscal Year 2019, Washington, DC, February 12, 2018, p. 274, https://www.govinfo.gov/content/pkg/BUDGET-2019-PER/pdf/BUDGET-2019-PER-7-8.pdf.

Notes: At the time that the FY2019 budget was being prepared, the FY2018 appropriations were incomplete and agencies were delayed in reporting the FY2017 outlays. The base discretionary column reflects the enacted appropriations and includes many post appropriation changes, such as transfers and rebasing.

Table 3. FY2018 Major Agency Cybersecurity Funding

Cybersecurity Funding Relative to Base Net Discretionary Budget Authority, in millions of nominal dollars

Agency	Base Discretionary (Estimate)	Cybersecurity Funding (Actual)	Cybersecurity Funding as a % of Base Discretionary
Agriculture	$22,500	$262	1.16%
Commerce	$9,300	$350	3.76%
Defense	$574,500	$8,048	1.40%
Education	$67,800	$104	0.15%
Energy	$30,000	$448	1.49%
HHS	$86,300	$359	0.42%
Homeland Security	$44,100	$1,859	4.22%
HUD	$47,700	$15	0.03%
Interior	$13,400	$88	0.66%
Justice	$28,100	$821	2.92%
Labor	$12,000	$93	0.78%
State	$38,100	$362	0.95%
Transportation	$19,200	$185	0.96%
Treasury	$12,600	$445	3.53%
Veterans Affairs	$77,300	$386	0.50%
EPA	$8,000	$21	0.26%
NASA	$19,500	$171	0.88%
NSF	$7,400	$247	3.34%
SBA	$800	$9	1.13%

Source: Office of Management and Budget, *Efficient, Effective, Accountable: An American Budget*, Fiscal Year 2019, Washington, DC, February 12, 2018, p. 144, https://www.govinfo.gov/content/pkg/BUDGET-2019-BUD/pdf/BUDGET-2019-BUD.pdf; Office of Management and Budget, *Analytic Perspectives*, Fiscal Year 2020, Washington, DC, March 18, 2019, p. 306, https://www.govinfo.gov/content/pkg/BUDGET-2020-PER/pdf/BUDGET-2020-PER-5-8.pdf.

Notes: The FY2020 budget did not include an accounting of the FY2018 actuals. Instead, the estimated budget from FY2019 is used. At the time that the FY2019 budget was being prepared, the FY2018 appropriations were incomplete. The base discretionary column reflects appropriations from the continuing resolutions and estimates for the complete year.

Table 4. FY2019 Major Agency Cybersecurity Funding

Cybersecurity Funding Relative to Base Net Discretionary Budget Authority, in millions of nominal dollars

Agency	Base Discretionary (Actual)	Cybersecurity Funding (Actual)	Cybersecurity Funding as a % of Base Discretionary
Agriculture	$24,400	$208	0.85%
Commerce	$11,600	$446	3.85%
Defense	$616,200	$8,527	1.38%
Education	$70,500	$119	0.17%
Energy	$30,200	$578	1.92%
HHS	$100,800	$522	0.52%
Homeland Security	$47,300	$2,591	5.48%
HUD	$53,800	$61	0.11%
Interior	$14,100	$104	0.74%
Justice	$30,800	$837	2.72%
Labor	$12,000	$87	0.72%
State	$48,200	$382	0.79%
Transportation	$26,500	$216	0.82%
Treasury	$15,000	$511	3.41%
Veterans Affairs	$86,600	$497	0.57%
EPA	$8,900	$42	0.47%
NASA	$21,500	$168	0.78%
NSF	$8,100	$246	3.04%
SBA	$700	$16	2.33%

Source: Office of Management and Budget, *A Budget for America's Future*, Fiscal Year 2021, Washington, DC, February 10, 2020, p. 123, https://www.govinfo.gov/content/pkg/BUDGET-2021-BUD/pdf/BUDGET-2021-BUD.pdf; Office of Management and Budget, *Analytic Perspectives*, Fiscal Year 2021, Washington, DC, February 10, 2020, p. 268, https://www.govinfo.gov/content/pkg/BUDGET-2021-PER/pdf/BUDGET-2021-PER-6-6.pdf.

Notes: The FY2021 budget included an accounting of FY2019 actual spending. These figures were used.

Table 5. FY2020 Major Agency Cybersecurity Funding

Cybersecurity Funding Relative to Base Net Discretionary Budget Authority, in millions of nominal dollars

Agency	Base Discretionary (Enacted)	Cybersecurity Funding (Estimate)	Cybersecurity Funding as a % of Base Discretionary
Agriculture	$23,800	$231	0.97%
Commerce	$12,900	$514	3.99%
Defense	$633,300	$10,075	1.59%
Education	$72,200	$166	0.23%
Energy	$38,500	$550	1.43%
HHS	$105,800	$476	0.45%
Homeland Security	$48,100	$2,574	5.35%
HUD	$56,500	$68	0.12%
Interior	$14,700	$121	0.83%
Justice	$32,400	$901	2.78%
Labor	$12,400	$92	0.74%
State	$47,700	$406	0.85%
Transportation	$24,800	$262	1.06%
Treasury	$15,500	$588	3.80%
Veterans Affairs	$92,700	$525	0.57%
EPA	$9,100	$33	0.36%
NASA	$22,600	$167	0.74%
NSF	$8,300	$226	2.73%
SBA	$800	$16	2.00%

Source: Office of Management and Budget, *A Budget for America's Future*, Fiscal Year 2021, Washington, DC, February 10, 2020, p. 123, https://www.govinfo.gov/content/pkg/BUDGET-2021-BUD/pdf/BUDGET-2021-BUD.pdf; Office of Management and Budget, *Analytical Perspectives*, Fiscal Year 2022, Washington, DC, May 28, 2022, p. 168, https://www.govinfo.gov/content/pkg/BUDGET-2022-PER/pdf/BUDGET-2022-PER-6-2.pdf.

Notes: The Department of Defense was excluded from the FY2022 Analytical Perspective. The FY2021 Analytical Perspective estimated number is used for this table.

Table 6. FY2021 Major Agency Cybersecurity Funding

Cybersecurity Funding Relative to Base Net Discretionary Budget Authority, in millions of nominal dollars

Agency	Base Discretionary (Enacted)	Cybersecurity Funding (Estimate)	Cybersecurity Funding as a % of Base Discretionary
Agriculture	$23,900	$223	0.93%
Commerce	$8,900	$472	5.30%
Defense	$703,700	$9,846	1.40%
Education	$73,000	$165	0.23%
Energy	$41,800	$711	1.70%
HHS	$108,400	$598	0.55%
Homeland Security	$54,900	$2,097	3.82%
HUD	$59,600	$81	0.14%
Interior	$15,000	$124	0.83%
Justice	$33,500	$934	2.79%
Labor	$12,500	$109	0.87%
State	$53,300	$320	0.60%
Transportation	$22,400	$334	1.49%
Treasury	$13,500	$653	4.84%
Veterans Affairs	$104,600	$472	0.45%
EPA	$9,200	$28	0.30%
NASA	$23,300	$155	0.67%
NSF	$8,500	$244	2.87%
SBA	$800	$17	2.13%

Source: Office of Management and Budget, *Budget of the U.S. Government*, Fiscal Year 2022, Washington, DC, May 28, 2021, p. 57, https://www.govinfo.gov/content/pkg/BUDGET-2022-BUD/pdf/BUDGET-2022-BUD.pdf; Office of Management and Budget, *Analytical Perspectives*, Fiscal Year 2022, Washington, DC, May 28, 2022, p. 168, https://www.govinfo.gov/content/pkg/BUDGET-2022-PER/pdf/BUDGET-2022-PER-6-2.pdf.

Notes: The Department of Defense was excluded from the FY2022 Analytical Perspective. The FY2021 Analytical Perspective estimated number is used for this table.

Table 7. FY2022 Major Agency Cybersecurity Funding

Cybersecurity Funding Relative to Base Net Discretionary Budget Authority, in millions of nominal dollars

Agency	Base Discretionary (Requested)	Cybersecurity Funding (Estimate)	Cybersecurity Funding as a % of Base Discretionary
Agriculture	$27,900	$229	0.82%
Commerce	$11,500	$422	3.67%
Defense	$715,000	$10,400	1.45%
Education	$102,800	$225	0.22%
Energy	$46,200	$793	1.72%
HHS	$133,700	$7,153	5.35%
Homeland Security	$54,900	$2,409	4.39%
HUD	$68,700	$76	0.11%
Interior	$17,400	$144	0.83%
Justice	$35,300	$1,241	3.52%
Labor	$14,200	$105	0.74%
State	$63,600	$447	0.70%
Transportation	$25,700	$345	1.34%
Treasury	$15,000	$829	5.53%
Veterans Affairs	$113,100	$450	0.40%
EPA	$11,200	$29	0.26%
NASA	$248,300	$187	0.08%
NSF	$10,200	$256	2.51%
SBA	$900	$17	1.89%

Source: Office of Management and Budget, *Budget of the U.S. Government*, Fiscal Year 2022, Washington, DC, May 28, 2021, p. 57, https://www.govinfo.gov/content/pkg/BUDGET-2022-BUD/pdf/BUDGET-2022-BUD.pdf; Office of Management and Budget, *Analytical Perspectives*, Fiscal Year 2022, Washington, DC, May 28, 2022, p. 168, https://www.govinfo.gov/content/pkg/BUDGET-2022-PER/pdf/BUDGET-2022-PER-6-2.pdf; Department of Defense, *Defense Budget Overview*, Fiscal Year 2022 Budget Request, Washington, DC, May 2021, p. 3-4, at https://comptroller.defense.gov/Portals/45/Documents/defbudget/FY2022/FY2022_Budget_Request_Overview_Book.pdf.

Notes: The Department of Defense was excluded from the FY2022 Analytical Perspective. Its FY2022 cybersecurity spending figure is drawn from its FY2022 Congressional Budget Justification.

Table 8. Cybersecurity Funding by Major Agencies as a Percentage of Their Base Discretionary Budgets

FY2017-FY2022

Agency	FY17	FY18	FY19	FY20	FY21	FY22	*AVERAGE*
Agriculture	0.50%	1.16%	0.85%	0.94%	0.93%	0.82%	0.87%
Commerce	2.94%	3.76%	3.85%	5.43%	5.30%	3.67%	4.16%
Defense	1.38%	1.40%	1.38%	1.59%	1.40%	1.45%	1.44%
Education	0.11%	0.15%	0.17%	0.17%	0.23%	0.22%	0.17%
Energy	1.23%	1.49%	1.92%	1.53%	1.70%	1.72%	1.60%
HHS	0.37%	0.42%	0.52%	0.51%	0.55%	5.35%	1.29%
Homeland Security	3.81%	4.22%	5.48%	3.35%	3.82%	4.39%	4.18%
HUD	0.03%	0.03%	0.11%	0.13%	0.14%	0.11%	0.09%
Interior	0.62%	0.66%	0.74%	0.72%	0.83%	0.83%	0.73%
Justice	2.59%	2.92%	2.72%	2.79%	2.79%	3.52%	2.89%
Labor	0.70%	0.78%	0.72%	0.81%	0.87%	0.74%	0.77%
State	0.66%	0.95%	0.79%	0.60%	0.60%	0.70%	0.72%
Transportation	0.96%	0.96%	0.82%	1.08%	1.49%	1.34%	1.11%
Treasury	3.61%	3.53%	3.41%	3.59%	4.84%	5.53%	4.08%
Veterans Affairs	0.52%	0.50%	0.57%	0.46%	0.45%	0.40%	0.48%
EPA	0.31%	0.26%	0.47%	0.32%	0.30%	0.26%	0.32%
NASA	0.75%	0.88%	0.78%	0.72%	0.67%	0.08%	0.64%
NSF	2.44%	3.34%	3.04%	2.90%	2.87%	2.51%	2.85%
SBA	2.44%	1.13%	2.33%	1.96%	2.13%	1.89%	1.98%
SSA	1.68%	1.80%	2.24%	2.35%	2.70%	2.71%	2.25%
AVERAGE	1.38%	1.52%	1.65%	1.60%	1.73%	1.91%	1.63%

Source: CRS analysis of agency budgets.

Congress may choose to direct agencies to change their cybersecurity spending. In evaluating resource levels for cybersecurity, Congress may choose to set a baseline for spending (e.g., 0.75% or 1.0% of the base discretionary budget). Minimum spending levels may help to improve the agency's overall cybersecurity investment and provide opportunities to address historically under-resourced projects. However, general requirements for cybersecurity spending are not a guarantee that additional investments will be appropriately spent, or that the investments will result in significant improvements to an agency's cybersecurity posture.

Identification of areas of greatest risk is crucial to developing cybersecurity investment strategies. The Trump Administration required OMB to evaluate and report on federal cybersecurity risk.[77]

[77] Office of Management and Budget, *Federal Cybersecurity Risk Determination Report and Action Plan*, May 2018, at https://www.whitehouse.gov/wp-content/uploads/2018/05/Cybersecurity-Risk-Determination-Report-FINAL_May-2018-Release.pdf.

Additionally, the agency IGs[78] and Government Accountability Office (GAO)[79] have evaluated cybersecurity risks at agencies. These documents can provide a framework for assessing current risk and provide potential options for increased investment.

Beyond required evaluations and periodic assessments, agencies may require assistance in evaluating cybersecurity risk and developing strategies to mitigate those risks. Executive Order 14028, *Improving the Nation's Cybersecurity*, directs certain agencies to provide the .gov domain with technical assistance, such as developing security principles for cloud services use; providing standards for supply chain security; and mandating cyber incident reporting.[80] This assistance from agencies like CISA, NIST, and OMB can provide an agency with justifications for future cybersecurity budget requests and resource requirements.

Minimum spending levels are in addition to the annual oversight Congress already exercises over agency budgets. Policymakers may also choose to direct agencies to submit further analysis on their IT and cybersecurity expenditures so that authorizers and appropriators can make more informed decisions on resourcing agencies for cybersecurity missions.

Require Shared Services

Concerning the risks federal agencies face in managing IT and the security risks to IT systems and information, Congress and the executive branch have taken actions to alleviate managerial deficiencies at agencies by promoting shared services among agencies. By using shared services, organizations seek to achieve cost-savings, consolidate expertise necessary for the services, and improve efficiencies and performance for those services.

Congress passed the Modernizing Government Technology Act (MGT Act; P.L. 115-91, Title X, Subtitle G), which established a government-wide fund and authorized agency-specific modernization funds. The funds are meant to address the funding uncertainty agencies face with the annual appropriations process by providing a dedicated source of multi-year funding for IT improvements. Allocations from these funds are prioritized for IT modernization efforts to purchase cloud services and services shared among multiple agencies. OMB provided additional guidance to agencies seeking to use or establish these funds.[81] While agency-specific funds are authorized, few agencies have received appropriations for those funds.[82] The American Rescue Plan Act of 2021 (P.L. 117-2) provided around $2 billion for federal IT and cybersecurity, of which $1 billion is available to the Technology Modernization Fund until the end of FY2025.

OMB directed agencies to consolidate certain capabilities with Memorandum 19-16 (M-19-16), *Centralized Mission Support Capabilities for the Federal Government*.[83] The memorandum

[78] For example, see Department of Veterans Affairs Office of Inspector General, *Federal Information Security Modernization Act Audit for Fiscal Year 2020*, Report #20-019727-104, Washington, DC, March 31, 2020, at https://www.va.gov/oig/pubs/VAOIG-20-01927-104.pdf.

[79] U.S. Government Accountability Office, *Veterans Affairs: VA Needs to Address Persistent IT Modernization and Cybersecurity Challenges*, GAO-20-719T, September 16, 2020, at https://www.gao.gov/assets/gao-20-719t.pdf.

[80] Executive Office of the President, "Improving the Nation's Cybersecurity," 86 *Federal Register* 26633-26647, May 12, 2021.

[81] Office of Management and Budget, *Implementation of the Modernizing Government Technology Act*, M-18-12, Washington, DC, February 27, 2018, at https://www.whitehouse.gov/wp-content/uploads/2017/11/M-18-12.pdf.

[82] U.S. Congress, House Committee on Oversight and Reform, Subcommittee on Government Operations, *FITARA 10.0*, 116th Cong., 2nd sess., August 3, 2020.

[83] Office of Management and Budget, *Centralized Mission Support Capabilities for the Federal Government*, M-19-16, April 26, 2019, at https://www.whitehouse.gov/wp-content/uploads/2019/04/M-19-16.pdf.

establishes a process for designating agencies as Quality Services Management Offices (QSMO). The Cybersecurity and Infrastructure Security Agency (CISA) was selected as the QSMO for cybersecurity and is offering capabilities to federal agencies to supplement or supplant their current capabilities.[84] CISA also offers federal agencies additional tools to help secure their IT systems, such as (1) the National Cybersecurity Protection System (NCPS),[85] which scans internet traffic coming into and out of federal agencies; and (2) the Continuous Diagnostics and Mitigation Program (CDM),[86] which scans agency networks to determine the hardware, software, users, and data on those networks and their vulnerabilities.

Congress may choose to direct the agencies to pursue use of more shared services. GAO and agency IGs have highlighted shortcomings in the federal agency management of IT systems.[87] While the responsibility to manage the IT risks to an agency ultimately lies with the agency head and their designees, an agency may lack the expertise to assess its IT risk and/or appropriate IT security solutions, or lack the funding necessary to implement desired changes. One way to address these issues is to shift the provisioning of cybersecurity services to another agency. CISA may provision technical capabilities for an agency, such as Domain Name System (DNS) resolution, security operations center services, and CDM. In this arrangement, CISA's expertise is used to acquire the capability while the agency retains responsibility for its security, so an agency can continue to apply specialized expertise to the newly provided tools. If policymakers opt to pursue this option, agency concerns may include funding arrangements (i.e., from a working capital fund, from the CISA budget, from the agency's budget, from an MGT Act fund, or a combination of these options) and the duration of an authorization to use shared services.

Require NextGen Cybersecurity Services

Many traditional cybersecurity tools are built around preventing unauthorized access at the perimeter of an agency's network. Tools such as firewalls; intrusion detection and prevention systems (IDS and IPS); and identify, credential, access management systems (ICAM) are predominantly deployed between an agency's internal resources and external resources (e.g., between an agency's headquarters local-area-network, or LAN, and the public internet). However, cybersecurity experts have touted next-generation cybersecurity tools as necessary to adequately combat the increased sophistication of adversaries in cyberspace. Some next-generation cybersecurity tools, discussed below in more detail, include endpoint detection and response (EDR) systems, highly adaptive cybersecurity services (HACS), and zero-trust architecture. These next-generation tools move away from applying security based on a prescribed set of rules or signatures and toward constantly assessing what normal and appropriate system behavior should be and rapidly identifying anomalous behavior and potential threats.

[84] Cybersecurity and Infrastructure Security Agency, "Cybersecurity Quality Services Management Office," website, at https://www.cisa.gov/cyber-qsmo.

[85] Cybersecurity and Infrastructure Security Agency, "National Cybersecurity Protection System," website, at https://www.cisa.gov/national-cybersecurity-protection-system-ncps.

[86] Cybersecurity and Infrastructure Security Agency, "Continuous Diagnostics and Mitigation," website, at https://www.cisa.gov/cdm.

[87] For example, see U.S. Government Accountability Office, *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges*, GAO-21-228, March 2021, https://www.gao.gov/assets/gao-21-288.pdf.

Endpoint Detection and Response

Traditional antivirus systems block potentially malicious code by matching indicators of that code (e.g., a hash value[88]) against a library of known malware. While this system helps to stop some attacks, it is trivial for adversaries to alter the indicators of their malware at scale and deploy seemingly unique attacks upon their victims. EDR systems seek to address the limitation of signature-based security systems with heuristic-based security. EDR systems install a small program on all of an organization's endpoints (e.g., host machines such as laptops and connected devices such as Wi-Fi access points) and services (e.g., cloud servers) to identify normal behavior by authorized users of those endpoints and services. Those data are combined with data from other endpoints to create an organization-wide view of the organization's network security. This combination of data requires high-performance computing and artificial intelligence systems to analyze data at wire-speed. As such, most of the processing of potential threats does not happen on the endpoint, but through a cloud service provider. If an EDR application detects anomalous and potentially malicious software or activities on an endpoint, it can automatically take actions to block it, report it, and look for it across other endpoints.

While agencies are free to pursue EDR capabilities through individual contracts, the federal government currently does not have a central EDR program. To address this, Executive Order 14028 directs CISA to recommend options for EDR implementation and to issue requirements to agencies on EDR use.

Cybersecurity experts do not argue that EDR is a comprehensive solution, but rather that it resolves current weaknesses in cybersecurity postures. For instance, if EDR solutions were deployed at federal agencies, it is likely that those systems would have detected and blocked the attempt by malware to contact command and control servers in the SolarWinds attack. A challenge to EDR deployment is ensuring that all networked devices are enrolled and covered by the EDR platform. If a networked device is not covered by the EDR service, then that becomes the weak point malicious actors will see to exploit.

Highly Adaptive Cybersecurity Services

The General Services Administration (GSA) provides government-wide contract vehicles to federal agencies. One area of GSA's contract offerings is highly adaptive cybersecurity services (HACS). HACS are proactive and reactive cybersecurity services, including risk and vulnerability assessments, security architecture reviews, continuous monitoring services, threat actor hunting, penetration testing, and incident response.[89] These services are designed to allow agencies greater visibility into their IT inventory, network operations, and cybersecurity posture by moving agencies from static assessments of cybersecurity risk to dynamic and continual assessments, allowing agencies to quickly identify risks and take steps to mitigate them.

HACS have previously been touted by cybersecurity experts as way to provide continual, current, and customized cybersecurity review and tools to IT administrators.[90] Their adoption provides

[88] A *hash value* is the function of an algorithm that computes a unique value on a data file that is used to identify that file. In this sense, a hash value can be considered a fingerprint for the message. For further information, see Elaine Barker, Miles Smid, and Dennis Branstand, "A Profile for U.S. Federal Cryptographic Key Management Systems," *NIST Special Publication 800-152*, October 2015, at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-152.pdf.

[89] General Services Administration, "Highly Adaptive Cybersecurity Services (HACS)," webpage, May 11, 2021, at https://www.gsa.gov/technology/technology-products-services/it-security/highly-adaptive-cybersecurity-services-hacs.

[90] Senator Sheldon Whitehouse, Representative Michael T. McCaul, Karen Evans, and Sameer Bhalotra, *From*

another set of tools to identify potential weakness in systems or existing malicious activity. However, HACS require advanced expertise in order to engage with the service, understand the results, and take action on the recommendations. These services are usually used by sophisticated organizations. If many organizations seek to use HACS, it may exacerbate existing cybersecurity workforce shortages.

Zero Trust

Gaining attention among federal cybersecurity managers is the concept of *zero trust*.[91] Zero trust architectures move away from protecting the boundary of an IT network and toward limiting access within a network and continually assessing whether or not a presented user is authorized to access a particular resource. Zero trust shifts security focus from the location of the system to the data or resource being accessed by the individual user regardless of its place. This philosophy inherently shifts the presumption that users and devices on a network are vetted to one that views users and devices as suspicious and requiring constant verification.

NIST defines *zero trust* as follows:

> Zero trust (ZT) provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised. Zero trust architecture (ZTA) is an enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a zero trust architecture plan.[92]

During testimony before the Senate Homeland Security and Governmental Affairs Committee on May 11, 2021, Acting CISA Director Brandon Wales touted zero trust as the future of federal IT architecture, which would require significant financial investment but also create significant barriers to adversaries seeking to penetrate and exploit federal IT and data.[93] Executive Order 14028 creates policy around the move to zero trust by requiring agencies to develop a plan to implement zero trust architecture.

Congress may choose to accelerate plans an agency has for moving toward next-generation cybersecurity services. In examining this option, Congress may choose to create statutory requirements for the agency, mandate reports to Congress on their adoption, or provide explicit resources to support their adoption. Congress may also target specific systems for next-generation cybersecurity services adoption, such as those related to the maintenance of sensitive citizen data or financial management systems.

Awareness to Action: A Cybersecurity Agenda for the 45th President, CSIS task force report, January 2017, at https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/170110_Lewis_CyberRecommendationsNextAdministration_Web.pdf.

[91] MeriTalk, "CIO Briefing Room: Zero Trust," webpage, May 14, 2021, at https://www.meritalk.com/news/cio-briefing-room/zerotrust/.

[92] National Institute of Standards and Technology, *Zero Trust Architecture*, NIST Special Publication 800-207, August 2020, at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

[93] U.S. Congress, Senate Committee on Homeland Security and Governmental Affairs, *Prevention, Response, and Recovery: Improving Federal Cybersecurity Post-SolarWinds*, 117th Cong., 1st sess., May 11, 2021, at https://www.hsgac.senate.gov/hearings/prevention-response-and-recovery-improving-federal-cybersecurity-post-solarwinds.

Congress has required agencies to implement cybersecurity requirements in addition to those broadly applicable to the federal government. For example, the data breach notification

requirement in the Veterans Affairs Information Security Act is in addition to the data loss notification requirements in FISMA and the Privacy Act of 1974.

Author Information

Chris Jaikaran
Analyst in Cybersecurity Policy

Disclaimer