United States Government Accountability Office

Report to Congressional Requesters

# INFORMATION TECHNOLOGY

# DHS Directives Have Strengthened Federal Cybersecurity, but Improvements Are Needed

Accessible Version

**February 2020**

**GAO-20-133**

February 2020

# INFORMATION TECHNOLOGY

## DHS Directives Have Strengthened Federal Cybersecurity, but Improvements Are Needed

GAO Highlights

Highlights of GAO-20-133, a report to congressional requesters

## Why GAO Did This Study

DHS plays a key role in federal cybersecurity. FISMA authorized DHS, in consultation with the Office of Management and Budget, to develop and oversee the implementation of compulsory directives—referred to as binding operational directives—covering executive branch civilian agencies. These directives require agencies to safeguard federal information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk. Since 2015, DHS has issued eight directives that instructed agencies to, among other things, (1) mitigate critical vulnerabilities discovered by DHS through its scanning of agencies' internet-accessible systems; (2) address urgent vulnerabilities in network infrastructure devices identified by DHS; and (3) better secure the government's highest value and most critical information and system assets.

GAO was requested to evaluate DHS's binding operational directives. This report addresses (1) DHS's process for developing and overseeing the implementation of binding operational directives and (2) the effectiveness of the directives, including agencies' implementation of the directive requirements. GAO selected for review the five directives that were in effect as of December 2018, and randomly selected for further in-depth review a sample of 12 agencies from the executive branch civilian agencies to which the directives apply.

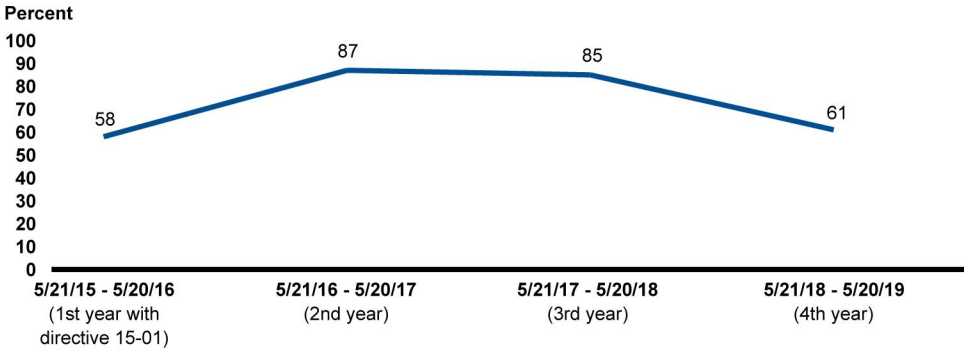
View GAO-20-133. For more information, contact Vijay A. D'Souza at (202) 512-6240 or dsouzav@gao.gov.

## What GAO Found

The Department of Homeland Security (DHS) has established a five-step process for developing and overseeing the implementation of binding operational directives, as authorized by the *Federal Information Security Modernization Act of 2014* (FISMA). The process includes DHS coordinating with stakeholders early in the directives' development process and validating agencies' actions on the directives. However, in implementing the process, DHS did not coordinate with stakeholders early in the process and did not consistently validate agencies' self-reported actions. In addition to being a required step in the directives process, FISMA requires DHS to coordinate with the National Institute of Standards and Technology (NIST) to ensure that the directives do not conflict with existing NIST guidance for federal agencies. However, NIST officials told GAO that DHS often did not reach out to NIST on directives until 1 to 2 weeks before the directives were to be issued, and then did not always incorporate the NIST technical comments. More recently, DHS and NIST have started regular coordination meetings to discuss directive-related issues earlier in the process. Regarding validation of agency actions, DHS has done so for selected directives, but not for others. DHS is not well-positioned to validate all directives because it lacks a risk-based approach as well as a strategy to check selected agency-reported actions to validate their completion.

Directives' implementation often has been effective in strengthening federal cybersecurity. For example, a 2015 directive on critical vulnerability mitigation required agencies to address critical vulnerabilities discovered by DHS cyber scans of agencies' internet-accessible systems within 30 days. This was a new requirement for federal agencies. While agencies did not always meet the 30-day requirement, their mitigations were validated by DHS and reached 87 percent compliance by 2017 (see fig. 1). DHS officials attributed the recent decline in percentage completion to a 35-day partial government shutdown in late 2018/early 2019. Nevertheless, for the 4-year period shown in the figure below, agencies mitigated within 30 days about 2,500 of the 3,600 vulnerabilities identified.

**Figure 1: Critical Vulnerabilities Mitigated within 30 days, May 21, 2015 through May 20, 2019**




Source: GAO analysis of Department of Homeland Security data. | GAO-20-133

Agencies also made reported improvements in securing or replacing vulnerable network infrastructure devices. Specifically, a 2016 directive on the *Threat to Network Infrastructure Devices* addressed, among other things, several urgent vulnerabilities in the targeting of firewalls across federal networks and provided technical mitigation

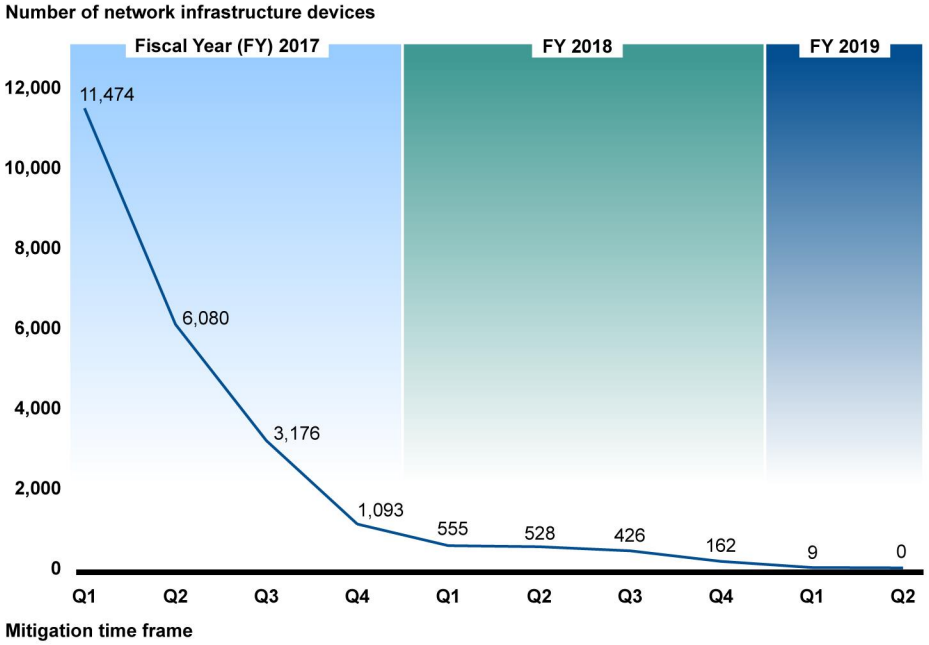
In addition, GAO reviewed DHS policies and processes related to the directives and assessed them against FISMA and Office of Management and Budget requirements; administered a data collection instrument to selected federal agencies; compared the agencies' responses and supporting documentation to the requirements outlined in the five directives; and collected and analyzed DHS's government-wide scanning data on government-wide implementation of the directives. GAO also interviewed DHS and selected agency officials.

## What GAO Recommends

GAO is making four recommendations to DHS: (1) determine when in the directive development process—for example, during early development and at directive approval—coordination with relevant stakeholders, including NIST, should occur; (2) develop a strategy for when and how to independently validate selected agencies' self-reported actions on meeting directive requirements, where feasible, using a risk-based approach; (3) ensure that the directive performance metric for addressing vulnerabilities identified in high value asset assessments aligns with the process DHS has established; and (4) develop a schedule and plan for completing the high value asset program reassessment and addressing the outstanding issues on completing the required assessments, identifying needed resources, and finalizing guidance to agencies and third parties. DHS concurred with GAO's recommendations and outlined steps and associated timelines that it planned to take to address the recommendations.

solutions. As shown in figure 2, in response to the directive, agencies reported progress in mitigating risks to more than 11,000 devices as of October 2018.

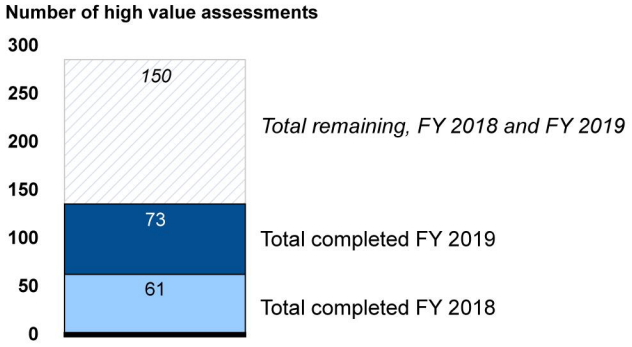
**Figure 2: Federal Civilian Agency Vulnerable Network Infrastructure Devices That Had Not Been Mitigated, September 2016 through January 2019**




Source: Department of Homeland Security data. | GAO-20-133

Another key DHS directive is *Securing High Value Assets,* an initiative to protect the government's most critical information and system assets. According to this directive, DHS is to lead in-depth assessments of federal agencies' most essential identified high value assets. However, an important performance metric for addressing vulnerabilities identified by these assessments does not account for agencies submitting remediation plans in cases where weaknesses cannot be fully addressed within 30 days. Further, DHS only completed about half of the required assessments for the most recent 2 years (61 of 142 for fiscal year 2018, and 73 of 142 required assessments for fiscal year 2019 (see fig. 3)). In addition, DHS does not plan to finalize guidance to agencies and third parties, such as contractors or agency independent assessors, for conducting reviews of additional high value assets that are considered significant, but are not included in DHS's current review, until the end of fiscal year 2020. Given these shortcomings, DHS is now reassessing key aspects of the program. However, it does not have a schedule or plan for completing this reassessment, or to address outstanding issues on completing required assessments, identifying needed resources, and finalizing guidance to agencies and third parties.

**Figure 3: Department of Homeland Security Assessments of Agency High Value Assets, Fiscal Years (FY) 2018 through 2019**




Source: GAO analysis of Department of Homeland Security data. | GAO-20-133

# Contents

Letter 1

Background 4
DHS Has Designed, but Not Fully Implemented, a Directive Process 13
Binding Operational Directives Often Have Been Effective in Addressing Cybersecurity Risks, but DHS Faces Challenges in Fulfilling Directive Requirements 18
Conclusions 38
Recommendations 38
Agency Comments and Our Evaluation 39

Appendix I: Objectives, Scope and Methodology 41

Appendix II: List of Federal Agencies to Which Binding Operational Directives Apply 45

Appendix III: Binding Operational Directives Process 50

Appendix IV: Binding Operational Directives and Associated Requirements 55

Appendix V: Technical Requirements Explanation for *Enhance Email and Web Security,* Binding Operational Directive 18-01 69

Appendix VI: Comments from the Department of Homeland Security 72

Appendix VII: GAO Contact and Staff Acknowledgments 77

Appendix VIII: Accessible Data 78

Data Tables 78
Agency Comment Letter 79

Tables

Table 1: Department of Homeland Security Binding Operational Directives and Their Issuance Dates 12
Table 2: Department of Homeland Security (DHS) Government-wide Binding Operational Directive (BOD) Critical

Vulnerability Mitigation Statistics, May 21, 2015 through May 20, 2019 20
Table 3: Department of Homeland Security Binding Operational Directive 18-01 Email Requirements 25
Table 4: Department of Homeland Security Binding Operational Directive 18-01 Web Requirements 26

Figures

Figure 1: Department of Homeland Security Binding Operational Directive (BOD), Percent of Critical Vulnerabilities Mitigated within 30 days, Government-wide and 12 Selected Agencies, May 21, 2015 through May 20, 2019 21
Figure 2: Federal Civilian Agency Progress in Mitigating Vulnerable Network Infrastructure Devices, September 2016 through January 2019 23
Figure 3: Department of Homeland Security Binding Operational Directive (BOD) 18-01 Government-wide Implementation across Domains by Directive Requirement, as of May 13, 2019 28
Figure 4: Compliance with Department of Homeland Security Binding Operational Directive 18-01 Email and Web Security Requirements in March 2018, October 2018, and May 2019 29
Figure 5: Department of Homeland Security Binding Operational Directive Life Cycle 54
Figure 1: Department of Homeland Security Binding Operational Directive (BOD), Percent of Critical Vulnerabilities Mitigated within 30 days, Government-wide and 12 Selected Agencies, May 21, 2015 through May 20, 2019 78
Figure 2: Federal Civilian Agency Progress in Mitigating Vulnerable Network Infrastructure Devices, September 2016 through January 2019 78
Figure 3: Department of Homeland Security Binding Operational Directive (BOD) 18-01 Government-wide Implementation across Domains by Directive Requirement, as of May 13, 2019 79
Figure 4: Compliance with Department of Homeland Security Binding Operational Directive 18-01 Email and Web Security Requirements in March 2018, October 2018, and May 2019 79

## Abbreviations

| | |
|---|---|
| BOD | binding operational directive |
| CFO Act | Chief Financial Officers Act of 1990 |
| CIO | chief information officer |
| CISO | chief information security officer |
| CISA | Cybersecurity and Infrastructure Security Agency |
| CSD | Cybersecurity Division |
| DHS | Department of Homeland Security |
| EINSTEIN | Department of Homeland Security cyber program |
| FISMA | Federal Information Security Modernization Act of 2014 |
| FNR | Federal Network Resilience Division |
| FedRAMP | Federal Risk and Authorization Management Program |
| GSA | General Services Administration |
| HVA | high value asset |
| HTTP | hypertext transfer protocol |
| HTTPS | hypertext transfer protocol secure |
| NASA | National Aeronautics and Space Administration |
| NCCIC | National Cybersecurity and Communications Integration Center |
| NIST | National Institute of Standards and Technology |
| NCATS | National Cybersecurity Assessments and Technical Services |
| OMB | Office of Management and Budget |
| RVA | risk and vulnerability assessment |
| SAR | security architecture review |
| US-CERT | U.S. Computer Emergency Readiness Team |

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

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

February 4, 2020

The Honorable Bennie G. Thompson
Chairman
Committee on Homeland Security
House of Representatives

The Honorable Cedric L. Richmond
Chairman
Subcommittee on Cybersecurity,
Infrastructure Protection, and Innovation
Committee on Homeland Security
House of Representatives

The Honorable Jim Langevin
House of Representatives

Federal agencies depend on information technology (IT) systems to carry out critical operations and to process essential data. However, the risks to these systems are increasing, including insider threats from malicious or unwitting employees, escalating cyber threats from around the globe, and the emergence of new and more destructive attacks. The federal government's development, implementation, and enforcement of policies that mitigate unauthorized access to these systems and unauthorized disclosure of the information they contain are vital to securing federal information systems.

Recognizing the importance of effective policies for securing federal information and systems, Congress passed the *Federal Information Security Modernization Act of 2014* (FISMA), which granted new authorities to the Department of Homeland Security (DHS) for administering the implementation of agency information security policies and practices.[1] Specifically, FISMA authorized the Secretary of Homeland

[1]*The Federal Information Security Modernization Act of 2014* (FISMA 2014), enacted as Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014), largely superseded the *Federal Information Security Management Act of 2002* (FISMA 2002), enacted as Title III, *E-Government Act of 2002*, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this report, FISMA refers to the new requirements in FISMA 2014, and to other relevant FISMA 2002 requirements that were unchanged by FISMA 2014 and continue in full force and effect.

Security, in consultation with the Director of the Office of Management and Budget (OMB), to develop and oversee the implementation of compulsory directives to federal civilian agencies—referred to as binding operational directives (directives). These directives require agencies to safeguard federal information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk. Since 2015, DHS has issued eight such directives to address vulnerabilities impacting federal civilian agencies.[2]

You asked us to review the development and implementation of the binding operational directives. The specific objectives of our review were to evaluate (1) DHS's process for developing and overseeing the implementation of binding operational directives and (2) the effectiveness of the binding operational directives, including agencies' implementation of the directive requirements.

To address the first objective, we reviewed DHS documentation, including policies and information on the department's process for developing, approving, and coordinating the binding operational directives. In addition, we reviewed requirements applicable to the directives contained in laws and guidance, including FISMA, and OMB memoranda M-19-03 and M-19-02.[3] We assessed DHS's written requirements and processes for developing and overseeing the implementation of the directives against these requirements and guidance. Further, we interviewed officials from DHS, OMB, and the National Institute of Standards and Technology (NIST) to obtain their views on the steps taken to develop and implement

[2]In addition to binding operational directives, DHS also has the authority to issue emergency directives in response to a known or reasonably suspected information security threat, vulnerability, or incident that represents a substantial threat to the information security of an agency. This authority was granted by the *Federal Cybersecurity Enhancement Act of 2015*. As of November 2019, only one emergency directive had been issued—*Mitigate DNS Infrastructure Tampering*, Emergency Directive 19-01. This emergency directive was not included in the scope of our review. The *Federal Cybersecurity Enhancement Act of 2015* is a part of the Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, div. N, title II, subtitle B, 129 Stat. 2242, 2963-2975 (Dec. 18, 2015).

[3]The White House, Office of Management and Budget, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*, M-19-03 (Washington, D.C.: Dec. 10, 2018); and The White House, Office of Management and Budget, *Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements*, M-19-02 (Washington, D.C.: Oct. 25, 2018).

the directives.[4] We also reviewed DHS's documentation on its process for evaluating agency actions to address the requirements in the directives.

To address the second objective, we randomly selected a sample of 12 agencies from the 99 civilian executive branch agencies to which the directives applied[5] and that reported actual cybersecurity expenditures of over $30 million in fiscal year 2017 (the most recent budget data available at the time we conducted our review).[6] We also selected five of the eight directives that had been issued (15-01, 16-02, 17-01, 18-01, and 18-02) for a more detailed review.[7] We selected these directives because they contained requirements that were still applicable as of December 2018, when we were planning our review and analysis.

We then developed and administered a data collection instrument to the selected agencies. As part of this process, we collected and reviewed agency documentation to determine actions agencies have taken to address directive requirements. We compared the agencies' responses and supporting documentation, such as compliance reports, corrective plans of action, and remediation plans, with the requirements outlined in the five directives.

[4]FISMA requires DHS to consult with NIST regarding any binding operational directive that implements standards and guidelines developed by NIST and ensure that the directives do not conflict with the standards and guidelines.

[5]Although there are more than 99 federal civilian agencies, DHS's Cybersecurity and Infrastructure Security Agency (CISA) tracks the compliance of 99 federal civilian agencies with respect to the binding operational directives. CISA officials note that this list of agencies will change in fiscal year 2020. See appendix II for the list of agencies that CISA tracks for compliance with directives. For a list of federal agencies, see the U.S. Government Manual 32 (2015)

[6]The 12 selected agencies were (1) Department of Education; (2) Department of Homeland Security; (3) Department of the Interior; (4) Department of Justice; (5) Department of the Treasury; (6) Federal Deposit Insurance Corporation; (7) Federal Retirement Thrift Investment Board; (8) General Services Administration; (9) National Aeronautics and Space Administration; (10) Securities and Exchange Commission; (11) Social Security Administration; and (12) Tennessee Valley Authority.

[7]Department of Homeland Security, *Critical Vulnerability Mitigation Requirement for Federal Civilian Executive Branch Departments and Agencies' Internet-Accessible Systems,* Binding Operational Directive 15-01 (Washington, D.C.: May 21, 2015); DHS, *Threat to Network Infrastructure Devices*, Binding Operational Directive 16-02 (Washington, D.C.: Sept. 27, 2016); DHS, *Removal of Kaspersky-branded Products,* Binding Operational Directive 17-01 (Washington, D.C.: Sept. 13, 2017); DHS, *Enhance Email and Web Security*, Binding Operational Directive 18-01 (Washington, D.C.: Oct. 16, 2017); DHS, *Securing High Value Assets*, Binding Operational Directive 18-02 (Washington, D.C:. May 7, 2018).

We reviewed DHS's reports on government-wide performance metrics and associated targets related to the directives' implementation. We then assessed the steps the department was taking to measure agencies' performance against DHS's established metrics and targets for the directives' implementation.

In addition, we reviewed the five directives and other relevant requirements, including OMB memoranda and DHS supplemental guidance on developing plans of action and milestones that outline specific reporting data, and a supplemental memorandum on high value asset reporting. We also collected and analyzed government-wide scanning data from DHS's National Cybersecurity and Communications Integration Center and DHS reports to Congress and OMB related to government-wide implementation of the directives. To assess the reliability of the scanning data and related DHS analysis that we used to support the findings in this report, we interviewed agency officials to determine the steps taken to ensure the integrity and reliability of the data and reviewed relevant documentation to substantiate the evidence obtained through interviews with agency officials. We determined that the data used in this report were sufficiently reliable for the purposes of our reporting objectives.

We supplemented our analyses with interviews of DHS and selected agency officials to obtain their views on the steps they have taken to address the directives. A more detailed discussion of our objectives, scope, and methodology can be found in appendix I.

We conducted this performance audit from October 2018 to February 2020 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

## Background

Federal agencies depend on computerized information systems and electronic data to process, maintain, and report essential information, and to operate and control physical processes. Virtually all federal operations are supported by computer systems and electronic data, and agencies would find it difficult, if not impossible, to carry out their missions and

account for their resources without these cyber assets. Hence, the security of these systems and data is vital to public confidence and the nation's safety, prosperity, and well-being.

However, computer networks and systems used by federal agencies can be riddled with security vulnerabilities—both known and unknown. These systems are often interconnected with other internal and external systems and networks, including the internet, thereby increasing the number of avenues of attack.

Cybersecurity incidents continue to impact federal entities and the information they maintain. According to DHS's U.S. Computer Emergency Readiness Team (US-CERT), agencies reported 31,107 information security incidents in fiscal year 2018.[8] These incidents involved several threat vectors, such as web-based attacks, phishing attacks, and the loss or theft of computer equipment, among others.[9] These incidents and others like them can pose a serious challenge to economic, national, and personal privacy and security.

Safeguarding federal computer systems has been a long-standing concern, with 2020 marking the 23rd anniversary since GAO first designated information security as a government-wide high-risk area.[10] We expanded this high-risk area to include safeguarding the systems supporting our nation's critical infrastructure in 2003, protecting the privacy of personally identifiable information in 2015, and establishing a comprehensive cybersecurity strategy and performing effective oversight in 2018.[11] Most recently, we continued to identify federal information

[8]Within DHS, US-CERT is a component of the National Cybersecurity and Communications Integration Center. It serves as the central federal information security incident center specified by FISMA.

[9]A threat vector (or avenue of attack) specifies the conduit or means used by the source or attacker to initiate a cyberattack, while phishing is a digital form of social engineering that uses authentic-looking, but fake, emails to request information from users or direct them to a fake website that requests information.

[10]GAO, *High-Risk Series: An Overview*, GAO/HR-97-1 (Washington, D.C.: February 1997) and GAO, *High-Risk Series: Information Management and Technology*, GAO/HR-97-9 (Washington, D.C.: February 1997).

[11]GAO, *High-Risk Series: An Update,* GAO-15-290 (Washington, D.C.: February 11, 2015) and *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation,* GAO-18-622 (Washington, D.C.: September 6, 2018).

security as a government-wide high-risk area in our March 2019 high-risk update.[12]

Beginning in fiscal year 2015 and continuing through fiscal year 2019, we made approximately 1,700 information security related recommendations. These recommendations identified actions for agencies to take to strengthen their information security programs and technical controls over their computer networks and systems. Nevertheless, many agencies continue to be challenged in safeguarding their information systems and information, in part, because they have not implemented many of these recommendations. As of the end of September 2019, approximately 650 of our prior information security related recommendations had not been implemented.[13]

## Federal Law and Policy Outline Key DHS Responsibilities in Securing Online Information and Systems

DHS plays a key role in the cybersecurity posture of the federal government and in the cybersecurity of systems that support the nation's critical infrastructures. Specifically, FISMA gave DHS responsibilities for administering the implementation of agency information security policies and practices for non-national security information systems, in consultation with OMB.[14]

One of DHS's responsibilities is to issue binding operational directives to federal civilian agencies that align with OMB's policies, principles,

[12]GAO, *High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas*, GAO-19-157SP (Washington, D.C.: March 6, 2019).

[13]To search for information on the status of prior GAO recommendations, go to GAO's Recommendation Database at https://www.gao.gov/reports-testimonies/recommendations-database.

[14]As defined in FISMA, the term "national security system" means any information system used by or on behalf of a federal agency that (1) involves intelligence activities, national security-related cryptologic activities, command and control of military forces, or equipment that is an integral part of a weapon or weapons system, or is critical to the direct fulfillment of military or intelligence missions (excluding systems used for routine administrative and business applications) or (2) is protected at all times by procedures established for handling classified national security information. See 44 U.S.C. § 3552(6)(A). For the purposes of this report, systems that do not meet the criteria for national security systems are referred to as non-national security systems.

standards, and guidelines. These directives apply to the federal civilian agencies that fall under DHS's FISMA authorities, but do not apply to national security systems or certain systems operated by the Department of Defense or the intelligence community.[15] See appendix II for a list of agencies to which the directives apply.

In introducing the authority to issue binding operational directives, the Senate report accompanying FISMA 2014[16] noted that OMB would continue to have federal information security enforcement responsibilities through its budget powers and its discretion in setting overarching information security policies. Accordingly, OMB has issued several memorandums regarding cybersecurity, including:

- OMB M-15-01, *Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices,* required DHS to perform regular scans of public facing segments of federal civilian agency networks for vulnerabilities on an ongoing basis, as well as in response to newly discovered vulnerabilities. OMB has since rescinded this memorandum and replaced it with guidance for fiscal year 2018-2019 (M-19-02).[17]
- OMB M-15-13, *Policy to Require Secure Connections Across Federal Websites and Web Services,* requires that all publicly accessible federal websites and web services only provide services through a

[15]Although there are more than 99 federal civilian agencies, DHS's Cybersecurity and Infrastructure Security Agency (CISA) tracks the compliance of 99 federal civilian agencies with respect to the binding operational directives. CISA officials note that this list of agencies will change in fiscal year 2020. See appendix II for the list of agencies that CISA tracks for compliance with directives. For a list of federal agencies, see the U.S. Government Manual 32 (2015).

[16]*Federal Information Security Modernization Act of 2014: Report of the Committee on Homeland Security and Governmental Affairs, United States Senate. To accompany S. 2521 to amend chapter 35 of title 44, United States Code, To Provide for Reform to Federal Information Security,* Committee on Homeland Security and Governmental Affairs, United States Senate, September 15, 2014.

[17]The White House, Office of Management and Budget, *Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices,* M-15-01 (Washington, D.C.: Oct. 3, 2014).

secure connection using hypertext transfer protocol secure[18] (HTTPS).[19]

- OMB M-19-02, *Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements,*[20] provides agencies with guidance and deadlines to comply with FISMA and reaffirms the value of agencies identifying and prioritizing their high value assets (HVA) as directed by DHS and OMB.[21]
- OMB M-19-03, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program,* expands the HVA program to support and provide guidance to both Chief Financial Officers Act (CFO Act)[22] and non-CFO Act agencies in HVA identification, assessment, remediation, and incident response.[23] Under M-19-03, an agency may designate federal information or a federal information system as a HVA when it falls under one or more of the following categories:

[18]Hypertext transfer protocol secure (HTTPS) is a combination of hypertext transfer protocol (HTTP) and transport layer security. It verifies the identity of a website or web service for a connecting client, and encrypts nearly all information sent between the website or service and the user.

[19]The White House, Office of Management and Budget, *Policy to Require Secure Connections Across Federal Websites and Web Services,* M-15-13 (Washington, D.C.: June 8, 2015).

[20] The White House, Office of Management and Budget, *Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements*, M-19-02 (Washington, D.C.: Oct. 25, 2018).

[21]A high value asset is a designation for federal information or a federal information system that is considered vital to an agency fulfilling its primary mission, or is considered essential to an agency's security and resilience.

[22]The 23 civilian *Chief Financial Officers Act of 1990* agencies are the Departments of Agriculture, Commerce, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Personnel Management; Small Business Administration; Social Security Administration; and the U.S. Agency for International Development.

[23]The White House, Office of Management and Budget, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*, M-19-03 (Dec. 10, 2018).

## DHS's Roles and Responsibilities for Binding Operational Directives

- **Informational Value.** The information, or the system that processes, stores, or transmits the information, is of high value to the federal government or its adversaries.
- **Mission Essential.** The agency that owns the information or information system cannot accomplish its primary mission essential functions, as approved in accordance with the National Continuity Policy, found in Presidential Policy Directive 40 (PPD-40),[24] within expected timelines without the information or information system.
- **Federal Civilian Enterprise Essential.** The information or information system serves a critical function in maintaining the security and resilience of the federal civilian enterprise.

Several entities within DHS have responsibilities for the binding operational directives. The department's Cybersecurity and Infrastructure Security Agency's (CISA) Cybersecurity Division is the lead entity for initiating, developing, issuing and overseeing the implementation of the directives.[25] CISA oversees the Federal Network Resilience (FNR) division and the National Cybersecurity and Communications Integration Center (NCCIC) in carrying out specific roles related to the directives.

**Federal Network Resilience.** FNR manages the coordination process for the directives, and oversees implementation of required actions at federal civilian agencies. To do so, FNR collects initial recommendations for new directives, drafts the directives, conducts agency outreach, and tracks agencies' implementation of the directives. FNR is to collaborate with OMB, NIST, the National Security Council, federal chief information

[24]The White House, *National Continuity Policy*, Presidential Policy Directive 40 (Washington, D.C.: July 15, 2016) directs the Secretary of Homeland Security through the Administrator of the Federal Emergency Management Agency to coordinate the implementation, execution, and assessment of continuity activities among executive departments and agencies.

[25]The *Cybersecurity and Infrastructure Security Agency Act of 2018*, Pub. L. 115–278, title XXII, 132 Stat. 4168-4186 (Jan. 3, 2018) renamed DHS's National Protection and Programs Directorate as the Cybersecurity and Infrastructure Security Agency and required that the new agency's director would report to the Secretary of DHS. The director's responsibilities include carrying out the cybersecurity and critical infrastructure activities of the agency, including binding operational directives.

officers (CIOs), and chief information security officers (CISOs) on cybersecurity risk management and operational governance and training; conduct operational assessments for agencies; and assist agencies in identifying areas to improve cybersecurity.

**National Cybersecurity and Communications Integration Center.** NCCIC is the federal civilian coordinator for information sharing concerning cybersecurity risks, incidents, analysis, and warnings with federal and nonfederal entities. The National Cybersecurity Assessments and Technical Services (NCATS), a group within NCCIC, conducts automated network and vulnerability scans of federal civilian agencies' internet-accessible systems to identify vulnerabilities and configuration errors. Based on these scans, NCATS produces weekly cyber hygiene reports for each agency. The weekly reports describe vulnerabilities detected, affected systems, and mitigation guidance. In addition to the weekly reports, since early June 2019, NCATS has provided agencies with daily notification of any newly detected critical and high severity vulnerabilities. NCATS also conducts reviews of agencies' high value assets, including security architecture and risk and vulnerability assessments on an ongoing basis.

### Other Federal Entities Assist in Coordinating Binding Operational Directives

In addition to the DHS components described previously, several other entities assist in coordinating the binding operational directive process. Specifically, DHS's FNR division coordinates with:

- **Chief information officers and the Federal CIO Council:** Federal agencies' CIOs and the council serve as a source of input for new directives. The council is the principal forum for improving agency practices related to the design, acquisition, development, modernization, use, sharing, and performance of federal information resources.
- **Chief information security officers and the Chief Information Security Officer Council:** Federal agencies' CISOs and the council discuss pending directives. The CISO Council, which is a subcommittee of the Federal CIO Council, collaborates to share information, transfer knowledge, and develop a unified approach to address federal IT security challenges.

- **Small Agency Council:** Members discuss pending directives and the potential impacts on small agencies. The council is a voluntary management association representing about 80 small agencies.[26]
- **National Institute of Standards and Technology (NIST):** NIST experts are to ensure that binding operational directives do not conflict with NIST standards and guidelines. NIST is responsible for developing standards and guidelines that include minimum information security requirements for federal agencies. To this end, NIST has issued guidance to agencies in implementing an information security program. For example, Security and Privacy Controls for Federal Information Systems and Organizations, NIST Special Publication 800-53, provides guidance to agencies on the selection and implementation of information security and privacy controls for systems.[27]
- **General Services Administration (GSA):** GSA coordinates with DHS and OMB, on an as-needed basis, to align cybersecurity services offered in its commercial IT contracts with DHS requirements for assessments, penetration testing, and additional cybersecurity services available to agencies, particularly related to HVAs.[28]

## Binding Operational Directives Address Known Cyber Threats, Risks, and Vulnerabilities

DHS developed and issued eight binding operational directives from May 2015 through April 2019 to address known cyber threats, risks, and

[26]The Small Agency Council is a voluntary management association of sub-Cabinet, independent federal agencies. Established in 1986, the council represents about 80 small agencies. The council meets periodically to discuss management issues of concern to small agencies.

[27]National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, SP 800-53, Rev. 4 (Gaithersburg, MD: April 2013) (updated January 2015).

[28]GSA established a highly adaptive cybersecurity services special item number on IT Schedule 70 (a long-term GSA contract issued to commercial IT vendors) to provide agencies quicker access to key cybersecurity support services from vendors. Those services include performing risk and vulnerability assessments and security architecture reviews on agencies' high value assets.

vulnerabilities. These directives instruct agencies to, among other things:[29]

- mitigate critical vulnerabilities discovered by DHS's NCCIC through its scanning of agencies' internet-accessible systems;[30]
- better secure their HVAs by participating in risk and vulnerability assessments (RVA)[31] and security architecture reviews (SAR)[32] conducted on their assets;[33] and
- address several urgent vulnerabilities in network infrastructure devices identified in a NCCIC analysis report.[34]

Table 1 provides a list of the directives and their issuance dates.

**Table 1: Department of Homeland Security Binding Operational Directives and Their Issuance Dates**

| Directive | Issue date |
|---|---|
| BOD 15-01–*Critical Vulnerability Mitigation Requirement for Federal Civilian Executive Branch Departments and Agencies' Internet-Accessible Systems* (revoked and replaced by BOD 19-02–*Vulnerability Remediation Requirements for Internet-Accessible Systems)* | May 21, 2015 |
| BOD 16-01–*Securing High Value Assets* (revoked and replaced by BOD 18-02 – *Securing High Value Assets*) | June 9, 2016 |

[29]Since their issuance, two binding operational directives have been revoked and replaced—BOD 16-01, *Securing High Value Assets*, revoked and replaced by BOD 18-02, and BOD 15-01, *Critical Vulnerability Mitigation Requirement for Federal Civilian Executive Branch Departments and Agencies' Internet-Accessible Systems*, revoked and replaced by BOD 19-02.

[30]BOD 19-02, *Vulnerability Remediation Requirements for Internet-Accessible Systems* (replaced BOD 15-01*, Critical Vulnerability Mitigation Requirement for Federal Civilian Executive Branch Departments and Agencies' Internet-Accessible Systems*).

[31]RVA is a service in which the assessor uses a number of techniques to identify weaknesses in the security posture of a given HVA. These techniques can include network mapping, vulnerability scanning, phishing tests, wireless assessments, web application assessments, and database assessments.

[32]For a SAR, the assessor analyzes the architecture of the HVA and develops recommendations for improving HVA security related to system design and interconnections.

[33]BOD 18-02, *Securing High Value Assets* (replaced BOD 16-01*, Securing High Value Assets*).

[34]BOD 16-02, *Threat to Network Infrastructure Devices* (approved as completed by DHS on March 1, 2019).

| | |
|---|---|
| BOD 16-02–*Threat to Network Infrastructure Devices* (closed by DHS, March 2019) | September 27, 2016 |
| BOD 16-03–*2016 Agency Cybersecurity Reporting Requirements* | October 17, 2016 |
| BOD 17-01–*Removal of Kaspersky-branded Products* (closed by DHS, July 2018) | September 13, 2017 |
| BOD 18-01–*Enhance Email and Web Security* | October 16, 2017 |
| BOD 18-02–*Securing High Value Assets* (replaced BOD 16-01 – *Securing High Value Assets*) | May 7, 2018 |
| BOD 19-02–*Vulnerability Remediation Requirements for Internet-Accessible Systems* (replaced BOD 15-01–*Critical Vulnerability Mitigation Requirement for Federal Civilian Executive Branch Departments and Agencies' Internet Accessible Systems*) | April 29, 2019 |

Source: GAO summary of Department of Homeland Security (DHS) data | GAO-20-133

# DHS Has Designed, but Not Fully Implemented, a Directive Process

DHS designed a process to develop and oversee the binding operational directives, but it has not followed key components of the process. Specifically, DHS has not involved stakeholders early in directive development and has not consistently overseen agencies' implementation of some directives through validation of reported results.

## DHS's Process for Developing and Implementing Directives

FISMA requires that DHS develop and oversee the implementation of binding operational directives to safeguard federal information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk and to implement the policies, principles, standards, and guidelines developed by the director of OMB, such as OMB memoranda M-19-03 and M-19-02.

Pursuant to FISMA, DHS designed and is using a draft process for developing and overseeing the implementation of cybersecurity binding operational directives. According to CISA officials, the department was to follow this process since issuance of the second directive on securing high value assets (BOD 16-01) in June 2016. In October 2017, DHS documented the process, which it has since updated. According to CISA officials, as of January 2020, this document was still in draft and was undergoing internal agency review.

According to the draft process, DHS is to engage in five steps to develop and implement binding operational directives (as discussed below and in more detail in appendix III):

1. **Identify** a potential directive topic and **determine** the extent to which it needs to be addressed. DHS's FNR is to identify topics for new directives from a wide variety of sources, including technical assessments, operational findings of cybersecurity issues, and discussions with external partners such as the Federal CIO Council, NIST, or OMB. FNR is to consider, among other things, whether or not a potential directive topic could be best addressed using the directive process, as well as considering its potential value and impact. Once a topic is identified, FNR officials are to conduct research on the topic and solicit feedback from stakeholders, such as DHS CISA representatives, federal agency chief information officers and chief information security officers, and relevant OMB, NIST, and GSA officials. Once the research is completed, FNR is to make a determination on whether to proceed in developing a directive.
2. **Develop** a draft directive, send it to relevant stakeholders for review, and obtain approval to issue it. After FNR officials develop the draft directive, they are to send it to relevant stakeholders (e.g. CISA, OMB, NIST, and the DHS Office of General Counsel) for a review of the scope and contents of the directives. FNR staff are to incorporate any feedback from stakeholders into the draft directive and then send it to the CISA director for approval and issuance.
3. **Distribute** the approved directive to all relevant agencies. FNR officials are to notify agencies of the directive's issuance via an email and a telephone call within 24 hours of the signing of the directive. In addition, FNR may choose to publicly post the directive to the DHS website. After FNR distributes the directive, agencies are to begin to address the directive's requirements.
4. **Implement and report** on agencies' efforts and progress in addressing the directive requirements. A CISA team is to review agency compliance with the directive through directive-related scans and compliance checks. The team is to distribute scorecards that indicate agency compliance with the directive requirements.
5. **Close out** the directive. DHS is to close a directive after it has validated that all of the requirements listed in the directive have been completed by all federal executive branch departments and agencies; the directive is no longer necessary because it has been revoked, suspended, or codified into law; or the directive needs to be amended.

## DHS Has Not Coordinated with Key Stakeholders Early in the Development Process

FISMA requires DHS to consult with NIST, consider NIST's standards and guidelines, and ensure that the directives it plans to implement do not conflict with NIST's established standards and guidelines. Consistent with this requirement, DHS's draft process calls for CISA to coordinate with stakeholders, such as NIST and GSA, early in the directive identification process to incorporate their input as a necessary part of executing the directive process.

CISA has not coordinated with key stakeholders early in the development process. According to NIST officials in the Information Technology Laboratory/Computer Security Division, which is responsible for working on directive issues, CISA coordinates with them to ensure that a new directive does not conflict with NIST guidance, but does not do so early in the process. Specifically, the NIST officials stated that often DHS did not reach out to NIST on the most recent directives until 1 to 2 weeks before they were to be issued, and then did not incorporate the NIST technical comments that were provided. As a result of the lack of timeliness in DHS's outreach to NIST, the directives may not include all key technical considerations.

In addition, CISA also has not coordinated with GSA on the directives early in the development process. For example, officials in GSA's Office of the Chief Information Officer told us that CISA did not coordinate with them on vendor issues before the directive on email and web security was issued.

CISA officials acknowledged that, in the past, the agency mainly relied on an ad hoc approach to coordination and did not always coordinate early in the planning process with stakeholders, including NIST and GSA, even though early coordination is called for in the current DHS process. CISA officials also explained that, in certain circumstances, they may need to accelerate the development process when a directive needs to be issued quickly due to elevated risk, such as the directive on addressing threats to

network devices in response to a specific hacking threat.[35] CISA officials told us that they have begun to have a more formalized coordination process with key stakeholders, including NIST and GSA. NIST officials also noted that DHS and NIST have started regular coordination meetings to discuss directive-related issues earlier in the process.

Nevertheless, CISA has yet to determine when in the directives' development—for example, during early development and at directive approval—coordination with specific entities should occur. Until CISA addresses this, a lack of effective coordination with stakeholders in the early stages of directives' development process and later in implementation is likely. This could result in directives that do not fully address key technical considerations, leaving agency systems at risk of being exposed to threats or vulnerabilities.

## CISA Has Not Validated Agencies Actions on All Directives

FISMA requires DHS to oversee agencies' implementation of its binding operational directives. To do this, DHS has outlined a process for validating agencies' reported results as part of the Close Out step of its directives process. As part of this process, CISA is supposed to validate that agencies have addressed all requirements before a directive is considered to be fully implemented. Guidance from OMB and executive orders also emphasize using a risk-based approach to information security. Specifically, to protect against cyber threats, agencies must make decisions about how to most effectively secure their systems and data, based on an assessment of the risks they face.

CISA has not validated agencies' actions on all five selected directives. Specifically, the agency validated the implementation of two directives by using cyber hygiene scanning[36] and provided weekly reports to the 99

[35]DHS noted in BOD 16-02, *Threat to Network Infrastructure Devices,* that the directive was issued in response to three particularly urgent issues—hacking tools targeting firewalls, Cisco Adaptive Security Appliance, and Cisco ROM Monitor Integrity—that required immediate attention across all impacted federal agencies. If these issues were not addressed, affected devices could compromise agencies' network infrastructure leading to increased risk of, among other things, denial-of-service attacks and data theft.

[36]Cyber hygiene scanning is comprised of vulnerability scanning on internet-accessible systems using a commercial tool as well as scanning for relevant web and email requirements using a software tool developed in house.

executive branch civilian agencies.[37] However, for the three other directives, CISA relied on agencies to self-report implementation and did not independently validate that the requirements had been met.[38]

According to CISA officials, the agency had to rely on agency submissions for these three directives because many of the potentially impacted devices were inside the agencies' networks and were not visible to CISA's scans, or were weaknesses identified in specific information security processes that CISA could not assess via scanning. For example, one directive required agencies to address vulnerabilities in specified network infrastructure devices internal to the network and then report to CISA either (1) completion of the actions, or (2) a plan of actions and milestones to complete the actions.[39] The officials added that it is the agency's responsibility to manage its own plan of actions and milestones, including verifications, and that they are not able to independently validate all of the actions because of a lack of an automated mechanism to detect findings inside agency networks and the lack of resources to do manual assessments.

While we recognize that CISA does not have the automated tools or capacity to independently validate every self-reported action taken by agencies to meet binding operational directive requirements, CISA can take a risk-based approach to validation. Guidance from OMB and executive orders emphasize risk-based approaches to information security. However, CISA did not take a risk-based approach, and it also did not have a strategy in place to check selected agency-reported actions to validate their completion. Without taking such an approach or having a strategy in place, the likelihood for requirements to not be completely or correctly addressed is increased. This could leave computer networks and systems used by federal agencies riddled with security vulnerabilities—both known and unknown.

[37]BOD 19-02, *Vulnerability Remediation Requirements for Internet-Accessible Systems* which replaced BOD 15-01*, Critical Vulnerability Mitigation Requirement for Federal Civilian Executive Branch Departments and Agencies' Internet-Accessible Systems,* and BOD 18-01, *Enhance Email and Web Security.*

[38]Specifically, BOD 16-02, *Threat to Network Infrastructure Devices;* BOD 17-01*, Removal of Kaspersky-branded Products; and* BOD 18-02, *Securing High Value Assets* which replaced BOD 16-01*, Securing High Value Assets.*

[39]BOD 16-02, *Threat to Network Infrastructure Devices.*

## Binding Operational Directives Often Have Been Effective in Addressing Cybersecurity Risks, but DHS Faces Challenges in Fulfilling Directive Requirements

Agencies' implementation of the directives has resulted in improvements that better safeguard federal information systems from a known or reasonably suspected information security threat, vulnerability, or risk. For example, according to DHS and agency data, in response to the directive on *Critical Vulnerability Mitigation* (BOD 15-01), agencies were able to mitigate about 2,500 out of about 3,600 critical vulnerabilities within 30 days of detection.[40]

However, not all agencies had been able to address all the directives' requirements within the required timelines established in four out of the five directives we reviewed. Moreover, DHS faced constraints in implementing the HVA program. Agencies and DHS cited a number of reasons for not fulfilling the requirements, including a lack of resources and technical expertise, as well as vendor constraints and operational issues. The five directives are discussed below and in more detail in appendix IV.

### Agencies Are Implementing Binding Operational Directives, but Not All Within Established Timelines

The civilian executive branch agencies to which the five selected binding operational directives apply are implementing and reporting on the requirements as called for in the directives. These five directives identify specific requirements to address known cyber threats, risks, and vulnerabilities and time frames for agency compliance, as well as requirements regarding how agencies are to report their progress on

[40]BOD 15-01, *Critical Vulnerability Mitigation Requirement for Federal Civilian Executive Branch Departments and Agencies' Internet-Accessible Systems*.

implementation of each directive to DHS.[41] However, not all agencies are doing so within the directives' established timelines (see directive details that follow).

## BOD 15-01: Mitigation of Critical Vulnerabilities on Internet-Accessible Systems Has Improved Since the Directive's Issuance

Issued on May 21, 2015, BOD 15-01, *Critical Vulnerability Mitigation* directed agencies to mitigate critical vulnerabilities discovered by DHS's NCCIC through cyber hygiene scans of agencies' internet-accessible systems. Agencies were to mitigate critical vulnerabilities within 30 days of NCCIC's notification. If agencies were unable to mitigate critical vulnerabilities within 30 days, they were to provide plans and status updates to DHS on a monthly basis until each vulnerability was fully addressed.[42]

According to DHS and agency data, since the directive issuance in 2015, the federal civilian agencies were able to mitigate about 2,500 out of about 3,600 critical vulnerabilities within 30 days of detection. Specifically, according to NCATS data, as of May 2018, the median number of days agencies were taking to mitigate critical vulnerabilities from the point of initial detection had been reduced from approximately 16 days (May 2015 to May 2016) to 6 days (from May 2017 to May 2018).[43] In addition, the agencies increased the percentage of critical vulnerabilities closed within 30 days of initial detection, from about 58 percent (May 2015 to May 2016) to 85 percent (from May 2017 to May 2018). See table 2 for more information on the critical vulnerability mitigation timeframes.

[41]Our review focused on binding operational directives 15-01, *Critical Vulnerability Mitigation Requirement for Federal Civilian Executive Branch Departments and Agencies' Internet-Accessible Systems*; 16-02, *Threat to Network Infrastructure Devices*; 17-01, *Removal of Kaspersky-branded Products*; 18-01, *Enhance Email and Web Security*; and 18-02, *Securing High Value Assets*.

[42]Critical vulnerabilities are typically remotely exploitable, are relatively simple to execute, use default or no authentication, and affect confidentiality, integrity, and availability. For example, the "Heartbleed" vulnerability, first identified in 2014, can be exploited to allow a remote user to retrieve information on user names and passwords in improperly patched systems.

[43]In the data we received, there are a few extreme values that tend to pull the average upward, making it not representative of the majority of values. Under these circumstances, median gives a better representation of central tendency than average.

**Table 2: Department of Homeland Security (DHS) Government-wide Binding Operational Directive (BOD) Critical Vulnerability Mitigation Statistics, May 21, 2015 through May 20, 2019**

| Critical vulnerability mitigation timelines | 5/21/15 through 5/20/16 (1st year with BOD 15-01) (Years since BOD 15-01 issuance) | 5/21/16 through 5/20/17 (2nd year with BOD 15-01) (Years since BOD 15-01 issuance) | 5/21/17 through 5/20/18 (3rd year with BOD 15-01) (Years since BOD 15-01 issuance) | 5/21/18 through 5/20/19 (4th year with BOD 15-01) (Years since BOD 15-01 issuance) |
|---|---|---|---|---|
| Critical vulnerabilities closed within 30 days of initial detection (percent) | 58 | 87 | 85 | 61 |
| Median time to close critical vulnerabilities (days) | 16 | 6 | 6 | 11 |
| Average time to close critical vulnerabilities (days) | 53 | 18 | 13 | 34 |

Source: DHS data. | GAO-20-133

Notes: According to DHS, the partial government shutdown during FY19 Q1-2 (lasting 35 days) affected closure rates, as many employees responsible for resolving vulnerabilities were furloughed.

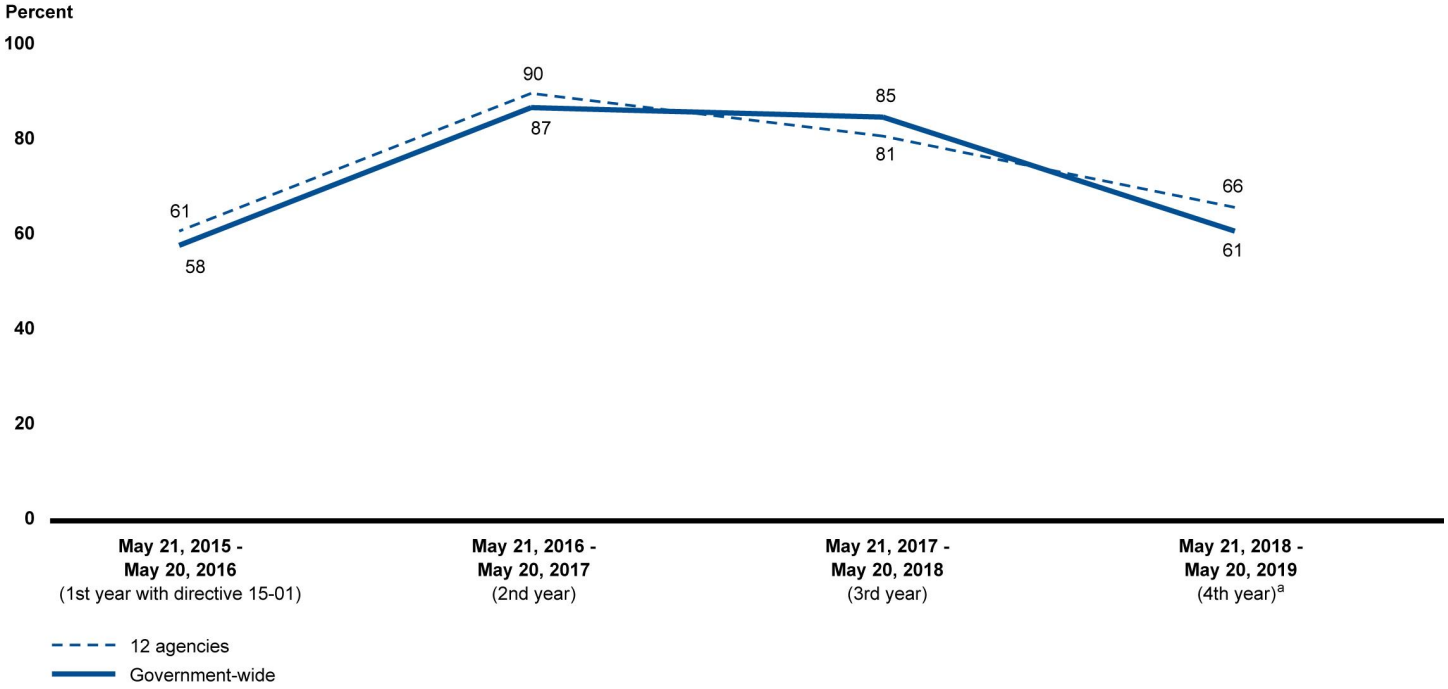
Percentages have been rounded to the nearest whole percent and days have been rounded to the nearest whole day.

In its fiscal year 2017 report to Congress on federal cybersecurity directives, DHS reported that the agencies were able to address vulnerabilities more quickly due, in part, to DHS setting clear expectations and timelines regarding mitigating critical vulnerabilities through its directive. Prior to the directive, there was no requirement for patching critical vulnerabilities within a certain time frame. As a result of the faster vulnerability mitigation, agencies are reducing the time their systems and networks are exposed to the cybersecurity risks associated with critical vulnerabilities.

In addition to the federal civilian agencies' improvements in critical vulnerability mitigation, the 12 selected agencies showed improvement in the average time needed to mitigate critical vulnerabilities. Specifically, in the third year after the directive issuance, according to NCATS data, four of the 12 selected agencies reported no critical vulnerabilities and five agencies reported a reduction in the average time needed to mitigate them. For example, one agency reduced the time it took to mitigate critical vulnerabilities from about 60 days to about 17 days on average. Further, all of the 12 selected agencies increased the percentage of critical vulnerabilities closed within 30 days of initial detection, from about 61 percent (from May 2015 to May 2016) to about 90 percent (from May 2016 to May 2017). While all covered agencies did not always meet the 30-day requirement, their mitigations were validated by DHS and reached 87 percent compliance by 2017. Officials attributed the recent decline in percentage mitigated to a 35-day partial government shutdown. Figure 1 provides information on the percent of critical vulnerabilities agencies

(federal civilian agencies and the 12 we reviewed) were able to mitigate within 30 days, as required under the directive.

**Figure 1: Department of Homeland Security Binding Operational Directive (BOD), Percent of Critical Vulnerabilities Mitigated within 30 days, Government-wide and 12 Selected Agencies, May 21, 2015 through May 20, 2019**




Source: GAO analysis of Department of Homeland Security data. | GAO-20-133

Notes: The 12 selected agencies were (1) Department of Education; (2) Department of Homeland Security; (3) Department of the Interior; (4) Department of Justice; (5) Department of the Treasury; (6) Federal Deposit Insurance Corporation; (7) Federal Retirement Thrift Investment Board; (8) General Services Administration; (9) National Aeronautics and Space Administration; (10) Securities and Exchange Commission; (11) Social Security Administration; and (12) Tennessee Valley Authority.

[a]According to DHS, the partial government shutdown during FY19 Q1-2 (lasting 35 days) affected closure rates, as many employees responsible for resolving vulnerabilities were furloughed.

In April 2019, DHS rescinded BOD 15-01 and replaced it with BOD 19-02, *Vulnerability Remediation Requirements for Internet-Accessible Systems.* This directive expands the requirements for agencies from addressing only critical vulnerabilities to addressing both critical and high vulnerabilities. Agencies are now required to mitigate critical vulnerabilities within 15 days of the vulnerabilities being identified through NCATS scanning (rather than within 30 days, as previously required), and to mitigate high vulnerabilities within 30 days of identification. According to the directive, if agencies are not able to mitigate the identified vulnerabilities in the required timeframes, they are to submit a

remediation plan to DHS outlining constraints, interim mitigation actions, and estimated completion dates.

## BOD 16-02: Federal Agencies Addressed Threats to Selected Network Infrastructure Devices, but Most Did Not Do So within the Established Timeline

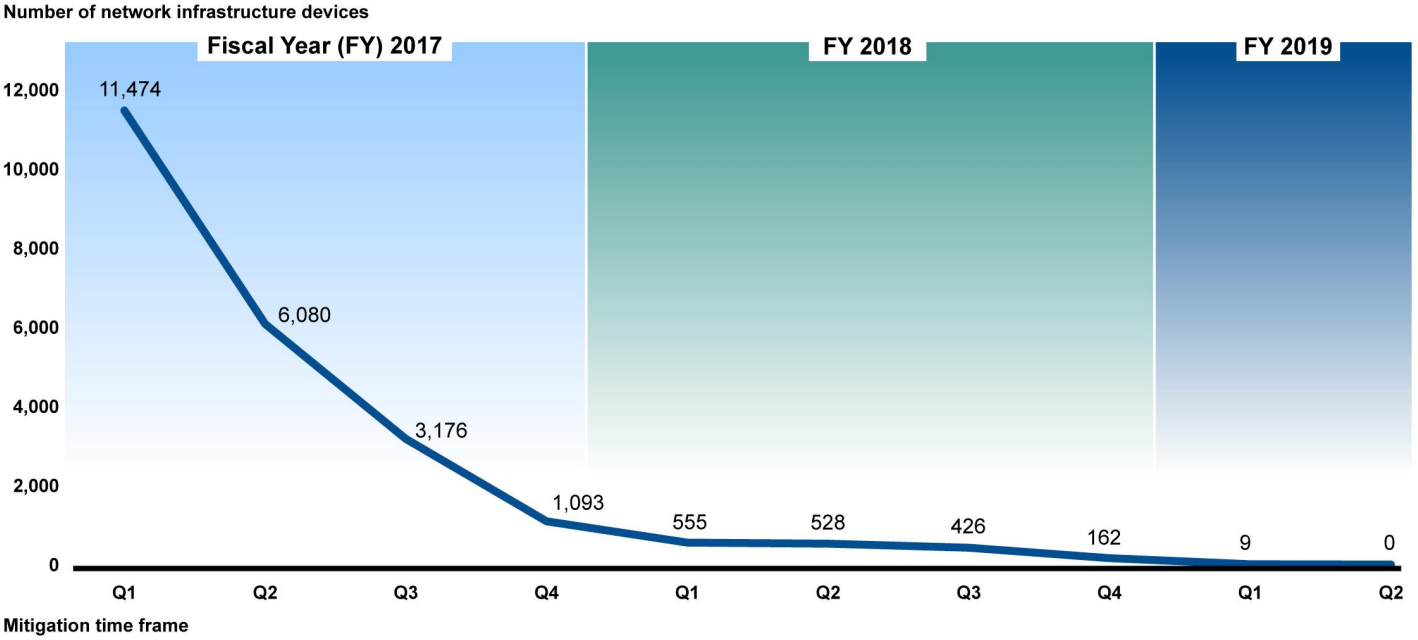
Issued on September 27, 2016, BOD 16-02, *Threat to Network Infrastructure Devices,* addressed several urgent vulnerabilities in network infrastructure devices identified in an August 2016 NCCIC report.[44] The report identified a known threat across federal networks and provided technical mitigation solutions. Specifically, it addressed hacking tools targeting firewalls, Cisco Adaptive Security Appliance devices, and devices running Cisco Internetwork Operating System (specifically the integrity of its ROM Monitor program). This directive required agencies to perform all mitigation actions identified in the NCCIC analysis report within 45 days, and to report either full mitigation or provide a detailed plan explaining constraints preventing mitigation. Agencies that were unable to achieve full mitigation within 45 days were instructed to provide monthly status updates until full mitigation was completed across their networks.

According to DHS's March 2019 report to OMB, within 6 months of issuance, the federal civilian agencies were able to remediate approximately 50 percent of impacted devices through patching and through upgrading outdated software. CISA reported that agencies completed all requested actions by October 2018, which was 2 years past the deadline.[45] According to CISA officials, agencies were not able to meet the timeline due to remediation challenges, such as replacing large amounts of end-of-life devices, replacing mission critical devices, and adjusting default configurations on impacted devices. While CISA did not independently validate agencies' actions in addressing the vulnerabilities as the devices were internal to the network, CISA reported that agencies secured over 11,000 network infrastructure devices across the federal civilian government (see figure 2).

[44]Department of Homeland Security, National Cybersecurity and Communications Integration Center, *The Increasing Threat to Network Infrastructure Devices and Recommended Mitigations,* AR-16-20173 (Washington, D.C.: Aug. 30, 2016).

[45]The DHS Secretary reviewed and approved the completion memorandum for BOD 16-02 on March 1, 2019.

**Figure 2: Federal Civilian Agency Progress in Mitigating Vulnerable Network Infrastructure Devices, September 2016 through January 2019**




Source: Department of Homeland Security data. | GAO-20-133

In addition to the federal civilian agencies' status, five of the 12 selected agencies reported full mitigation of the risks outlined in the directive requirements within the 45-day deadline (November 14, 2016). An additional five agencies did not report full mitigation within 45 days, but provided detailed plans of action and milestones to DHS every 30 days thereafter until full mitigation, as required. These five agencies had completion dates ranging from April 2017 to October 2018. The remaining two agencies were unable to demonstrate that they had completed the directive requirements. However, DHS reported that the covered federal civilian agencies were able to complete all actions associated with this directive by October 2018.

## BOD 17-01: Agencies Removed Risky Software Products from Their Information Systems in Response to a Stated Threat

Issued on September 13, 2017, BOD 17-01, *Removal of Kaspersky-branded Products*, required federal civilian agencies to (1) determine whether the agency had Kaspersky-branded products on its information systems within 30 days (October 13, 2017); (2) develop a plan to remove such products from its information systems within 60 days (November 13,

2017); and (3) begin implementing its plan for removal within 90 days (December 13, 2017) and provide DHS with updates every 30 days until the products were fully removed from agency information systems.[46]

According to DHS's fiscal year 2017 report to Congress, by April 2018, officials from federal civilian agencies had either attested that Kaspersky-branded products were not present on their information systems or removed such products, as required by the directive. Similarly, officials at the 12 selected agencies stated and reported that they performed the required analysis to identify the use or presence of Kaspersky-branded products and reported to DHS by the 30-day deadline (October 13, 2017). Of these, 10 agencies reported that they did not find the use or presence of Kaspersky-branded products in its information systems. One agency found Kaspersky-branded products in its systems but removed the product before the 60-day planning deadline. The remaining agency identified the use or presence of Kaspersky-branded products in its information systems and developed a detailed plan of action and provided status reports to DHS every 30 days until completion on December 6, 2017. Subsequently, these requirements were enacted into law in the *National Defense Authorization Act for Fiscal Year 2018*, which further prohibited federal agencies from using products and services developed or provided by Kaspersky Labs.[47]

[46]In a statement issued by DHS on September 13, 2017, DHS noted a concern "about the ties between certain Kaspersky officials and Russian intelligence and other government agencies, and requirements under Russian law that allow Russian intelligence agencies to request or compel assistance from Kaspersky and to intercept communications transiting Russian networks. The risk that the Russian government, whether acting on its own or in collaboration with Kaspersky, could capitalize on access provided by Kaspersky products to compromise federal information and information systems directly implicates U.S. national security." "Kaspersky-branded products" are information security products, solutions, and services supplied, directly or indirectly, by AO Kaspersky Lab or any of its predecessors, successors, parents, subsidiaries, or affiliates, including Kaspersky Lab North America, Kaspersky Lab, Inc., and Kaspersky Government Security Solutions, Inc. (collectively, "Kaspersky''). The directive did not address Kaspersky code embedded in the products of other companies.

[47]*National Defense Authorization Act for Fiscal Year 2018,* Pub. L. No. 115-91, § 1634, 131 Stat. 1283, 1739-41 (Dec. 12, 2017).

## BOD 18-01: Agencies Have Made Progress on Most Email and Web Security Requirements, but Many Have Yet to Fully Address the Requirements

Issued on October 16, 2017, BOD 18-01, *Enhance Email and Web Security*, required agencies to implement specific security standards that have been widely adopted in industry to ensure the integrity and confidentiality of internet-delivered data, minimize spam, and better protect users who might otherwise fall victim to a phishing email that appears to come from a government-owned system.[48] As such, this directive required several actions related to email and web security with three different due dates: within 90 days (by January 2018), within 120 days (by February 2018), and within 1 year (by October 2018). Tables 3 and 4 outline the email and web security requirements and appendix V provides more detailed information on these requirements.

**Table 3: Department of Homeland Security Binding Operational Directive 18-01 Email Requirements**

| Timeline | Directive requirements |
|---|---|
| Within 90 days (by January 15, 2018) | 1. Configure all internet-facing mail servers to offer STARTTLS, which makes passive man-in-the-middle attacks more difficult.<br>2. Start to incrementally strengthen email authentication by increasing DMARC policy requirements. |
| Within 120 days (by February 13, 2018) | 3. Strengthen encryption of emails by ensuring old SSL versions, SSLv2 and SSLv3, are disabled on mail servers.<br>4. Further strengthen encryption by ensuring legacy cipher suites, 3DES and RC4, are disabled on mail servers. |
| Within 1 year (by October 16, 2018) | 5. Further strengthen email authentication by setting a DMARC policy of “reject” for all second-level domains and mail-sending hosts to completely block delivery of unauthenticated messages. |

Source: GAO analysis of Department of Homeland Security, BOD 18-01 *Enhance Email and Web Security*. | GAO-20-133

Note: DHS issued a temporary exception for the 3DES weak cipher requirement for agencies dependent on email vendors to disable the weak cipher.

STARTTLS, an extension to plain text authentication protocols, which when enabled will signal to a sending mail server that the capability to encrypt an email in transit is present.

DMARC (domain-based message authentication, reporting and conformance) tells a recipient what the domain owner would like done with the message when an email is received that does not pass an agency’s posted SPF/DKIM rules. SPF (sender policy framework) and DKIM (domain keys identified

[48]Phishing is a digital form of social engineering that uses authentic-looking, but fake, emails to request information from users or direct them to a fake website that requests information.

mail) allow a sending domain to effectively “watermark” its emails, making unauthorized emails easy to detect.

SSL (secure sockets layer) is a computing protocol that ensures the security of data sent via the internet by using encryption.

3DES (data encryption standard), is an implementation of the data encryption standard (DES) algorithm that uses three passes of the DES algorithm instead of one as used in ordinary DES applications. Triple DES provides much stronger encryption than ordinary DES, but it is less secure than advanced encryption standard.

RC4 (Rivest Cipher 4) is a stream cipher algorithm that is used in popular protocols such as SSL (to protect internet traffic) and WEP (to secure wireless networks).

DMARC policy of “reject” provides the strongest protection against spoofed email, ensuring that unauthenticated messages are rejected at the mail server, even before delivery.

Domains are unique identifying addresses assigned to internet-accessible systems (such as .gov or dhs.gov).

**Table 4: Department of Homeland Security Binding Operational Directive 18-01 Web Requirements**

| Timeline | Directive requirements |
|---|---|
| Within 120 days (by February 13, 2018) | 1. Secure connections across all publicly accessible federal websites and web services by enforcing the use of HTTPS and HSTS.<br>2. Strengthen web security by ensuring old SSL versions, SSLv2 and SSLv3, are disabled on web servers.<br>3. Further strengthen web security by ensuring legacy cipher suites, 3DES and RC4, are disabled on web servers.<br>4. Further securing connections across all publicly-accessible Federal websites and web services by preloading second-level domains, which enforces the use of HTTPS on domains and allows agencies to avoid inventorying and configuring an HSTS policy for every individual subdomain. |

Source: GAO analysis of Department of Homeland Security, BOD 18-01 *Enhance Email and Web Security*, and follow-up documentation. | GAO-20-133

Note: STARTTLS = an extension to plain text communication protocols; SPF = sender policy framework; DMARC = domain-based message authentication, reporting and conformance; SSL = secure sockets layer; 3DES and RC4 ciphers = Rivest Cipher 4 (RC4), a stream cipher, and triple data encryption standard (3DES), a block cipher.

Hypertext transfer protocol (HTTP) connections can be easily monitored, modified, and impersonated.

HTTPS remedies each HTTP vulnerability.

HTTP strict transport security (HSTS) ensures that browsers always use an https:// connection, and removes the ability for users to click through certificate-related warnings.

SSL (secure sockets layer) is a computing protocol that ensures the security of data sent via the internet by using encryption.

3DES (data encryption standard), is an implementation of the data encryption standard (DES) algorithm that uses three passes of the DES algorithm instead of one as used in ordinary DES applications. Triple DES provides much stronger encryption than ordinary DES, but it is less secure than advanced encryption standard.

RC4 (Rivest Cipher 4) is a stream cipher algorithm that is used in popular protocols such as SSL (to protect internet traffic) and WEP (to secure wireless networks).

Domains are unique identifying addresses assigned to internet facing systems (such as .gov or dhs.gov).

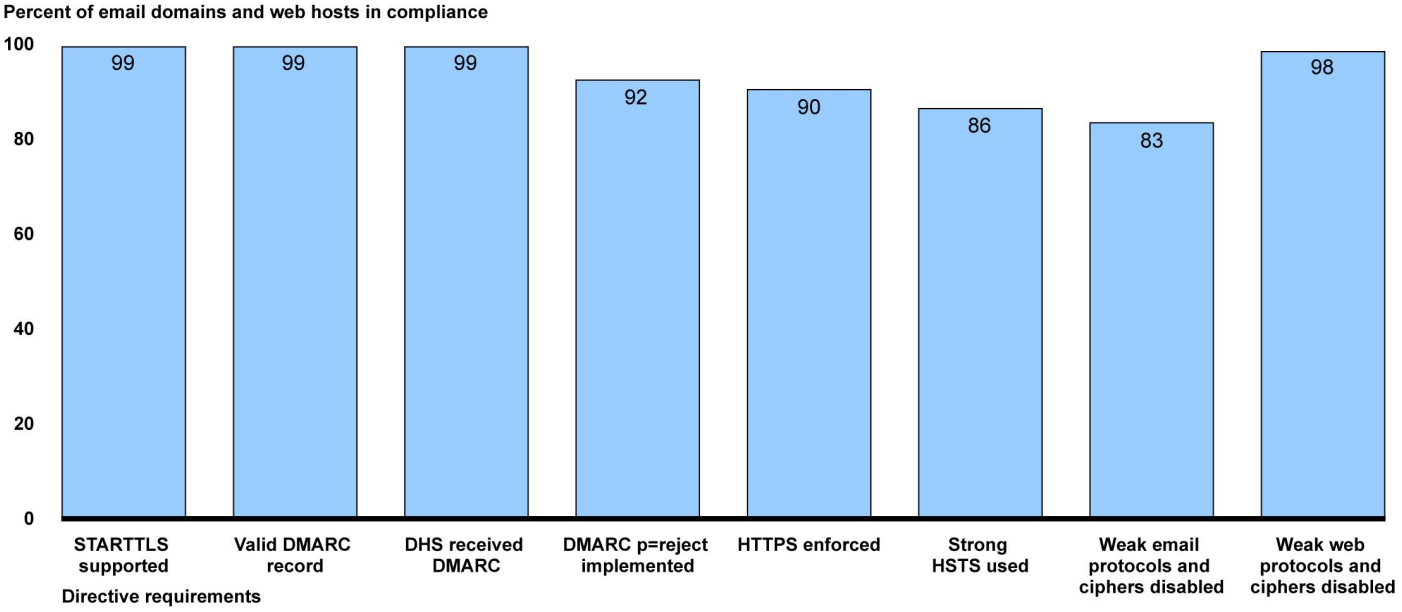
The federal civilian agencies had made significant progress in addressing individual email and web security requirements of the directive. However, few agencies had fully addressed all of the directive's email and web security requirements for all domains. A domain is a unique identifying address assigned to an internet-accessible system such as .gov or dhs.gov, and an individual agency may have multiple domains. NCATS scans each agency domain and measures it against the individual email and web requirements.[49] According to our analysis of NCATS' May 2019 scanning data, the agencies were between about 83 to 99 percent complete in addressing each individual email and web requirement across all domains (see figure 3).[50] Similarly, three of the 12 selected agencies, were 100 percent complete in addressing each individual email and web requirement for all domains. In addition, the remaining nine agencies' domains were from about 82 to almost 100 percent complete in addressing the individual email and web requirements.[51]

[49]A domain or domain name can be used to identify internet-accessible information systems, such as .gov (top level domain) and dhs.gov (second-level domain).

[50]To be included in the analysis, agencies had to be listed in NCATS' March 26, 2018, October 17, 2018, and May 13, 2019 Cyber Exposure Scorecards. In the data sets, some agencies did not have available data, had entries noted as not applicable, or did not have detectable email domains. These agencies were excluded in our analysis and a total of 83 agencies were included in our analysis. Further, the number of internet services and devices tested during an NCATS scan varies as agencies continue to expand their internet presence through increased deployment of internet-accessible systems and removal of some old systems. These additional domains must satisfy the directive's requirements. If the requirements are not implemented when the domain is scanned, an agency can fall out of compliance.

[51]The number of email domains and web hosts varied widely among the agencies. For example, as of May 13, 2019, one of the 12 agencies had two email domains and 10 web hosts, whereas another agency had 262 email domains and 2,848 web hosts.

**Figure 3: Department of Homeland Security Binding Operational Directive (BOD) 18-01 Government-wide Implementation across Domains by Directive Requirement, as of May 13, 2019**




STARTTLS (an extension to plain text authentication protocols), DMARC (domain-based message authentication, reporting and conformance), HTTPS (hypertext transfer protocol secure), HSTS (hypertext transfer protocol strict transport security), protocols (secure sockets layer version 2 (SSLv2) and 3 (SSLv3)), and ciphers RC4 (Rivest cipher 4), a stream cipher, and 3DES (triple data encryption standard), a block cipher

Source: GAO analysis of Department of Homeland Security (DHS) federal civilian agencies' data. | GAO-20-133

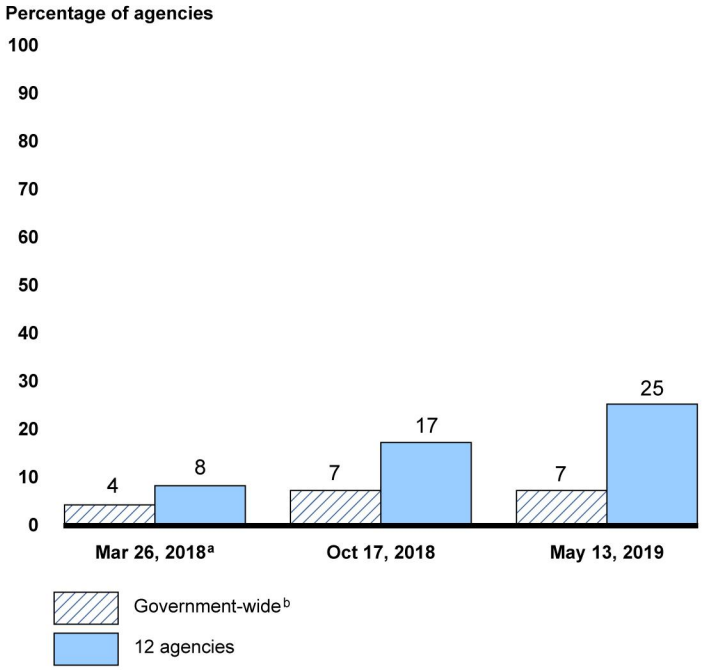
However, according to NCATS' March 2018 agency scanning data, only three of 83 agencies (4 percent) had fully addressed all of the directive's email and web security requirements due within the 120 day deadline across all of their domains.[52] Within 1 year of issuance, according to NCATS' October 2018 scanning data, six of 83 agencies (7 percent) had fully addressed all directive requirements. According to NCATS' May 2019 scanning data, three additional agencies fully addressed the requirements. However, three agencies had fallen out of compliance (leaving the total compliance rate at 7 percent).

Compliance with the email and web security requirements was slightly better for the 12 selected agencies. According to NCATS' March 2018 scanning data, one of the 12 selected agencies fully addressed the

[52]As noted earlier, we included only the agencies that were listed in all three of the following of NCCIC's Cyber Exposure Scorecards: March 26, 2018, October 17, 2018, and May 13, 2019.

directive's requirements due at the 120 day deadline (8 percent). Within 1 year of issuance, according to NCATS' October 2018 scanning data, one additional agency fully addressed the requirements (17 percent). According to NCATS' May 2019 scanning data, three of the 12 agencies fully addressed the requirements (25 percent). See figure 4 for details.

**Figure 4: Compliance with Department of Homeland Security Binding Operational Directive 18-01 Email and Web Security Requirements in March 2018, October 2018, and May 2019**




Source: GAO analysis of Department of Homeland Security data. | GAO-20-133

Note: The 12 agencies selected for GAO review were: (1) Department of Education; (2) Department of Homeland Security; (3) Department of the Interior; (4) Department of Justice; (5) Department of the Treasury; (6) Federal Deposit Insurance Corporation; (7) Federal Retirement Thrift Investment Board; (8) General Services Administration; (9) National Aeronautics and Space Administration; (10) Securities and Exchange Commission; (11) Social Security Administration; and (12) Tennessee Valley Authority.

[a]Agencies are considered compliant if they have met all deadlines before or on the dates listed. For March 26, 2018, one requirement was omitted because the deadline was after this date.

[b]To be included in the analysis, agencies had to be listed in NCCIC's March 26, 2018, October 17, 2018, and May 13, 2019 Cyber Exposure Scorecards. In the data sets, some agencies did not have available data, had entries noted as not applicable, or did not have detectable email domains. These agencies were excluded in our analysis and a total of 83 agencies were included in our analysis.

One of the key challenges that agencies have experienced in implementing the directive's email requirements is related to strengthening email security by disabling the 3DES weak email cipher. Specifically, according to CISA's March 2019 report to OMB, more than 50 agencies are dependent on email vendors that do not allow agencies to disable the 3DES cipher. FNR officials stated that after several agencies informed them of having vendor constraints, DHS started to work with vendors on behalf of the agencies. As a result, DHS issued a temporary exception in September 2018, 7 months after the initial deadline, for those agencies encountering this vendor constraint.

According to CISA's March 2019 report to OMB, in February 2019, one of the vendors began retiring the weak email cipher 3DES, but has not set a firm timeline on when it will be fully retired. In a June report to OMB, DHS stated that another email vendor had released a tool that agencies could implement to address the requirement to remove the weak email cipher 3DES. As of the end of April 2019, seven of the 12 selected agencies were affected by this vendor issue. CISA officials noted that they are working with industry officials, including at a leadership level, to ensure they understand when 3DES will be fully disabled. Once that happens, CISA reported that they will provide agencies with any additional support needed to address vendor management issues and the associated email and web requirements.

Additionally, FNR officials stated that many agencies struggled to implement a DMARC-related requirement on their systems due to its complexity. FNR officials noted that they have provided agencies with training through a non-profit organization and hosted a variety of outreach events, including presentations, to help agencies work through the complexity of implementing DMARC.

## BOD 18-02: Agencies Are Participating in DHS-led Assessments, but DHS and Agencies Have Not Been Able to Complete the Assessments and Mitigations in a Timely Manner

Issued on May 7, 2018, the purpose of BOD 18-02, *Securing High Value Assets*, is to enhance DHS's approach to secure the federal government's high value assets (HVAs) from cybersecurity threats.[53] It replaces an earlier directive[54] and requires agencies to:

1. Identify and submit coordination points of contact for HVA assessments within 7 days of issuance of the directive.
2. Submit a current and prioritized HVA list inclusive of all agency components within 30 days of issuance of the directive and review the agency HVA list and provide quarterly updates to DHS.[55]
3. Participate in DHS-led assessments of HVAs, if selected.
4. Ensure identified major or critical weaknesses are mitigated within 30 days of receipt of the risk and vulnerability assessment (RVA) reports and/or security architecture review (SAR); notify DHS that each identified weakness was addressed; and report the status of any remaining major or critical weaknesses to DHS every 30 days until full remediation.[56]

As stated earlier, in an RVA, the assessor uses a number of techniques to identify weaknesses in the security posture of a given HVA; for a SAR, the assessor analyzes the architecture of the HVA and develops recommendations for improving HVA security related to system design and interconnections. Techniques for RVA assessments can include network mapping, vulnerability scanning, phishing tests, wireless assessments, web application assessments, and database assessments. A SAR provides a holistic analysis of how an HVA's individual security components integrate and operate, including how data is protected during

[53]As noted earlier, a HVA is a designation for federal information or a federal information system that is considered vital to an agency fulfilling its primary mission, or is considered essential to an agency's security and resilience.

[54]BOD 16-01, *Securing High Value Assets*.

[55]While agencies are principally responsible for designating their HVAs, OMB and DHS may also designate HVAs at agencies based on potential impact to national security.

[56]A major or critical weakness is defined as a critical or high severity vulnerability identified in RVA reports and major or critical weaknesses identified in SAR reports.

operations. According to a DHS report to OMB, assessments can identify HVA weaknesses that require significant network design changes and extended timelines to resolve.

In December 2018, OMB issued a memorandum that expanded the definitions of HVAs, instructed agencies to prioritize their HVAs, and instructed agencies to conduct assessments of HVAs as directed by DHS.[57] Subsequently, CISA issued supplemental guidance for BOD 18-02 that divided HVAs into three tiers based on criticality and impact. The guidance defined Tier 1 systems as systems of critical impact to both the agency and the nation; Tier 2 systems as ones that have a significant impact on both the agency and the nation; and Tier 3 systems as those with a high impact on the agency. In addition, the supplemental guidance outlined the following required reviews:

- Tier 1 HVAs require one RVA and one SAR to be led by DHS every 3 years,
- Tier 2 HVAs require one RVA and one SAR to be conducted by an independent assessor or third party every 3 years, and
- Tier 3 HVAs require one RVA and one SAR agency self-assessment every 3 years.

In response to the directive and supplemental guidance, most of the federal civilian agencies have taken several steps to address the requirements, including identifying points of contact; submitting current and prioritized HVA lists, if appropriate; participating in DHS-led assessments if selected; and beginning to address identified weaknesses. Specifically, CISA's October 2019 data showed that federal civilian agencies have reported a total of 851 HVAs (212 Tier 1 and 639 Tier 2 and Tier 3 systems). In addition, CISA's October 2019 data showed that at the beginning of October 2019, DHS had conducted 61 assessments in fiscal year 2018 and 73 in fiscal year 2019. This includes a mix of both RVAs and SARs.

DHS has also taken steps to identify major or critical weaknesses from the HVA assessments. Specifically, CISA's October 2019 data showed

[57]As explained previously in this report, a high value asset (HVA) is information or an information system that is of high value to the federal government or its adversaries (informational value), or is considered vital to an agency fulfilling its primary mission (mission essential) or essential to an agency's security and resilience (federal civilian enterprise essential).

that, as of the end of September 2019, the 134 assessments identified 196 major or critical weaknesses.

DHS and the agencies have not completed the required assessments and mitigations consistent with OMB guidance and DHS policy. To address the review requirement for Tier 1 HVAs in accordance with the OMB and DHS-defined frequency of assessments, DHS should complete at least a total of 142 assessments a year. However, DHS completed only about half of the required annual assessments this year (with 73 assessments completed in fiscal year 2019).

In addition, DHS has yet to issue the guidance, standards, and methodologies for Tier 2 or Tier 3 HVA assessments, which are to be conducted by third parties and agencies, respectively. As a result, agencies cannot begin conducting assessments for the remaining 639 HVA systems.

Further, agencies have not been able to mitigate the identified weaknesses within the required timeframes. Specifically, CISA's October 2019 data showed that of the 196 major or critical weaknesses identified government-wide, agencies were not able to mitigate 160 within the required initial 30-day time frame; 75 major or critical weaknesses were still not mitigated as of early October 2019. Similarly, for the 12 selected agencies we reviewed, CISA's October 2019 data showed that as of early October, the department performed a total of 58 assessments, which resulted in the discovery of 86 major or critical weaknesses. However, 64 of these major or critical weaknesses were not mitigated within the required initial 30-day time frame, and 32 major or critical weaknesses were still not mitigated as of early October 2019.

In addition to the above requirements, DHS established a government-wide performance metric for agencies to address 45 percent of critical/high severity weaknesses discovered through HVA assessments within 30 days of them being reported, as required by the directive. However, DHS reported that agencies were only addressing these weaknesses within 30 days about 30 percent of the time. According to DHS, this shortcoming is largely due to the variety and difficulty of weaknesses identified by affected agencies in each calendar quarter, as well as the different maturity levels of agencies in addressing these weaknesses.

Further, the performance metric for addressing the HVA weaknesses is not fully aligned with the directive's requirements. Specifically, while the

directive states that agencies should address weaknesses within 30 days, the directive also states that if the senior accountable officer for risk management at the agency determines that a risk cannot be adequately addressed within 30 days, the agency must develop and submit a remediation plan to DHS for its review.[58] However, DHS's metric does not provide for such an option.

In implementing this directive, DHS recognized the need to measure the extent to which agencies are addressing the requirements and, therefore, improving government-wide cybersecurity. However, without a performance metric that is aligned with the binding operational directive process DHS has established, it will be challenged in demonstrating the overall efficacy of a binding operational directive in achieving cybersecurity goals.

## Agencies Identified Challenges Meeting Directive Timelines While DHS Faced Constraints in Implementing the HVA Assessment Program

Agency and DHS officials reported that agencies faced technical and resource challenges in addressing the various directive requirements within established timelines. This is consistent with challenges reported by officials at the 12 selected agencies. DHS has recognized these challenges and taken actions on them. However, DHS faces a variety of challenges in implementing the HVA program that remain outstanding.

### Agencies Reported Various Challenges in Meeting Timelines

Agencies reported various challenges in addressing the directive requirements within the established timelines. The challenges included (1) outdated systems that require costly updates or replacements before they can be brought into full compliance; (2) the lack of specialized expertise to address technical requirements; (3) the complexity of

[58]The senior accountable officer for risk management is either the agency head or a designated official. Per OMB's memo, if the agency head delegates this authority, the individual must be a direct report to the agency head, have visibility into all areas of the organization, particularly those focused on risk management, possess authority for both funding and management of information technology and enterprise risk, and be able to represent the challenges and opportunities across the enterprise.

achieving full DMARC compliance; and (4) general issues associated with addressing weaknesses in agency HVAs.

To address the first and second challenges (outdated systems and specialized expertise), in its March 2019 report to OMB, DHS provided the following considerations for OMB: (1) examine agency budgets to ensure agencies are deploying all available resources and capabilities against threats to government networks and data; (2) provide supplemental funds to agencies to support implementation of current and future binding operational directives; and (3) examine agency budgets to ensure agencies are deploying all available resources to obtain specialized training for staff or to hire specialized skill sets. According to CISA officials, OMB has contacted agencies that listed budget as a constraint in their plan of action and milestones and is currently discussing how OMB can provide assistance.

DHS has also provided support to agencies in addressing the third challenge on DMARC. For example, CISA officials stated that they offer webinars focused on DMARC implementation to those agencies that do not have necessary technical expertise.

With regard to the fourth challenge on HVAs, DHS reported that agencies government-wide faced a variety of challenges in addressing the weaknesses in their HVA programs, including issues with network segmentation and vulnerability to phishing attacks. In general, according to DHS, these types of weaknesses may not be easy to address within the required 30 days because they require long term planning and training, system or device procurement, and system integration and testing.

The 12 selected agencies concurred with DHS's view of the challenges they faced in addressing outstanding weaknesses associated with their HVAs. For example, one agency reported an enterprise-level deficiency related to an HVA that requires significant changes to its network design, with a projected remediation timeline of over a year in its plan of action and milestones. Another agency stated that it was unable to fully address a critical weakness within the DHS 30-day timeline, but did develop a remediation plan for the weakness and reported its progress to DHS as appropriate. In addition, another agency reported that it did not fully address a weakness within 30 days and also did not submit the required monthly reports. DHS reported that it has established an HVA Community of Interest with federal civilian agencies to identify and promote best

practices within agencies and improve the security and privacy posture of HVA systems.

Continued support from OMB and DHS in addressing the technical and resource constraints facing the agencies in addressing the requirements set in the directives will allow agencies to react quickly, efficiently, and effectively to the requirements of the directives.

## DHS Has Encountered Challenges in Fulfilling Its Responsibilities for the HVA Assessment Program

While OMB guidance and DHS policy are clear on DHS's responsibilities and time frames for the directive on the HVA program (BOD 18-02), DHS has yet to complete its HVA activities in a timely manner. Specifically, the HVA program manager within CISA stated that the department did not have sufficient resources to do all of the required assessments. As noted earlier, thus far, DHS has only conducted about half of the annual assessments required in DHS's own supplemental guidance. The official stated that the department was now reassessing the prioritization and planning process of the HVA program.

Further, CISA officials reported that they do not expect to issue the guidance, standards, and methodologies on Tier 2 and 3 HVAs until at least the end of fiscal year 2020. However, agencies cannot begin conducting Tier 2 third-party or Tier 3 agency self-assessments on HVA systems until DHS develops and issues the guidance, standards, and methodologies for these reviews, potentially leaving these critical systems at risk.

Moreover, a CISA official stated that DHS will need to work with GSA to add qualified contractors for Tier 2 assessments to the appropriate GSA contract vehicle.[59] The official stated that there is an ongoing effort with GSA to get contractors for third-party assessments certified by DHS added to the GSA schedule.

According to DHS officials from the HVA office, the department is now reassessing key aspects of the program. However, it does not have a schedule or plan for completing this reassessment, or to address outstanding issues on completing required assessments, identifying needed resources, and finalizing guidance to agencies and third parties. Without such a schedule and plan, agencies may continue to face prolonged cybersecurity threats.

[59]OMB, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*, M-19-03, requires DHS to work with GSA to add qualified contractors into the highly adaptable cybersecurity services (HACS) special item number (SIN) on GSA's IT Schedule 70, which agencies can then use to solicit services for Tier 2 assessments.

## Conclusions

Although DHS has designed a process to develop and oversee the implementation of binding operational directives, it is not following all the steps in the draft process. Specifically, the department has not involved key stakeholders, such as NIST and GSA, early in the process. Additionally, although guidance from OMB and executive orders emphasize risk-based approaches to information security, CISA did not take such an approach in validating selected agency-reported actions. Until DHS addresses the coordination and validation issues, the likelihood is increased that directives will not fully address key technical considerations and requirements are not fully addressed.

Federal civilian agencies have made many significant improvements in cybersecurity by implementing the directives' requirements. However, an important performance metric for addressing vulnerabilities identified by HVA assessments does not align with the process DHS has established. Further, DHS has only completed about half of the required assessments for fiscal year 2019. In addition, DHS does not plan to issue the guidance, standards, and methodologies on Tier 2 and 3 systems until at least the end of fiscal year 2020. Given these shortcomings, DHS has been reassessing key aspects of the HVA program. However, there was no schedule or plan for completing the HVA reassessment and for addressing the outstanding issues on completing the required assessments, identifying needed resources, and finalizing guidance for Tier 2 and 3 systems. Without such a schedule and plan, agencies may continue to face increased and prolonged cybersecurity threats.

## Recommendations

We are making four recommendations to the Department of Homeland Security:

The Secretary of Homeland Security should determine when in the directive development process—for example, during early development and at directive approval—coordination with relevant stakeholders, including NIST and GSA, should occur. (Recommendation 1)

The Secretary of Homeland Security should develop a strategy to independently validate selected agencies' self-reported actions on

meeting binding operational directive requirements, where feasible, using a risk-based approach. (Recommendation 2)

The Secretary of Homeland Security should ensure that the binding operational directive performance metric for addressing vulnerabilities identified by high value asset assessments aligns with the process DHS has established. (Recommendation 3)

The Secretary of Homeland Security should develop a schedule and plan for completing the high value asset program reassessment and addressing the outstanding issues on completing the required high value asset assessments, identifying needed resources, and finalizing guidance for Tier 2 and 3 HVA systems. (Recommendation 4)

## Agency Comments and Our Evaluation

We provided a draft of this report to DHS for review and comment. We also provided informational copies of the report to the other agencies involved in the review: OMB; NIST; the Departments of Education, the Interior, Justice, and the Treasury; the Federal Deposit Insurance Corporation; the Federal Retirement Thrift Investment Board; the General Services Administration; the National Aeronautics and Space Administration; the Securities and Exchange Commission; the Social Security Administration; and the Tennessee Valley Authority.

In written comments (reproduced as appendix VI), DHS agreed with our recommendations and described steps planned or under way to address them. For example, in its written response, DHS noted that the department is working to formalize a risk-based strategy to validate agency results with an estimated completion date of September 30, 2020. It also added that the department is working with OMB to address the need for independent validation. DHS and NIST also provided technical comments on the draft report, which we incorporated as appropriate.

We are sending copies of this report to the appropriate congressional committees and the Acting Secretary of Homeland Security. In addition, the report will be available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-6240 or at dsouzav@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on

the last page of this report. GAO staff who made key contributions to this report are listed in appendix VII.

Vijay A. D'Souza
Director, Information Technology and Cybersecurity

# Appendix I: Objectives, Scope and Methodology

Our objectives were to evaluate (1) the Department of Homeland Security's (DHS) process for developing and overseeing the implementation of binding operational directives (directives) and (2) the effectiveness of the directives, including agencies' implementation of directive requirements.

To address our first objective, we reviewed DHS documentation, including its policies and process information related to departmental development, approval, and coordination of the directives.[1] We also reviewed DHS written requirements and process for overseeing how agencies are implementing the directives. In addition, we reviewed requirements from law and guidance including the *Federal Information Security Management Act of 2014* (FISMA),[2] and memoranda from the Office of Management and Budget (OMB).[3] We evaluated DHS's process against these

[1]In addition to binding operational directives, DHS also has the authority to issue emergency directives in response to a known or reasonably suspected information security threat, vulnerability, or incident that represents a substantial threat to the information security of an agency. This was authorized by the *Federal Cybersecurity Enhancement Act of 2015*. As of November 2019, only one emergency directive has been issued—*Mitigate DNS Infrastructure Tampering*, Emergency Directive 19-01. The emergency directive was not included in the scope of this review.

[2]The *Federal Information Security Modernization Act of 2014* (FISMA 2014), enacted as Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014), largely superseded the *Federal Information Security Management Act of 2002* (FISMA 2002), enacted as Title III, *E-Government Act of 2002*, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this report, FISMA refers to the new requirements in FISMA 2014, and to other relevant FISMA 2002 requirements that were unchanged by FISMA 2014 and continue in full force and effect.

[3]The White House, Office of Management and Budget, *Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices,* M-15-01 (Washington, D.C.: Oct. 3, 2014); The White House, Office of Management and Budget, *Policy to Require Secure Connections Across Federal Websites and Web Services,* M-15-13 (Washington, D.C.: June 8, 2015); The White House, Office of Management and Budget, *Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements*, M-19-02 (Washington, D.C.: Oct. 25, 2018); and The White House, Office of Management and Budget, *Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program*, M-19-03 (Washington, D.C.: Dec. 10, 2018).

requirements. Further, we interviewed officials from DHS, OMB, and National Institute of Standards and Technology (NIST) to obtain their views and verify the information provided.

To address our second objective we selected five binding operational directives that had active requirements at the time we were designing our review and analysis in December 2018. These were:

- BOD 15-01, *Critical Vulnerability Mitigation Requirement for Federal Civilian Executive Branch Departments and Agencies' Internet-Accessible System,* issued May 21, 2015. (This directive was revoked and replaced by BOD 19-02, *Vulnerability Remediation Requirements for Internet-Accessible Systems* in April 2019.)
- BOD 16-02, *Threat to Network Infrastructure Devices* (designated as closed by DHS, March 2019), issued September 27, 2016
- BOD 17-01, *Removal of Kaspersky-branded Products*, issued September 13, 2017
- BOD 18-01, *Enhance Email and Web Security*, issued October 16, 2017
- BOD 18-02, *Securing High Value Assets*, issued May 7, 2018

We then randomly selected a sample of 12 agencies from the civilian executive branch agencies,[4] to which DHS directives apply, to determine the extent to which these agencies have taken steps to address the directives' requirements.[5] Specifically, we randomly selected agencies from among those that had reported actual cybersecurity expenditures of over $30 million in fiscal year 2017 (the most recent data available at the time we began our review).

The 12 selected agencies were (1) Department of Education; (2) Department of Homeland Security; (3) Department of the Interior; (4) Department of Justice; (5) Department of the Treasury; (6) Federal Deposit Insurance Corporation; (7) Federal Retirement Thrift Investment

[4]Although there are more than 99 federal civilian agencies, DHS's Cybersecurity and Infrastructure Security Agency (CISA) tracks the compliance of 99 federal civilian agencies with respect to the binding operational directives. See appendix II for list of agencies that CISA tracks for compliance with directives. For a list of federal agencies, see the U.S. Government Manual 32 (2015).

[5]We chose $30 million as the cutoff, as this would provide a list of agencies for which the impact of our findings/recommendations could be the greatest and those that may have the resources to address these findings/recommendations.

Board; (8) General Services Administration; (9) National Aeronautics and Space Administration; (10) Securities and Exchange Commission; (11) Social Security Administration; and (12) Tennessee Valley Authority.

We developed a data collection instrument based on the directives' requirements. We administered the data collection instrument to the selected agencies and collected supporting documentation, such as compliance reports, corrective plans of action/plans of actions and milestones, and remediation plans and responses to the requirements outlined in five directives (15-01, 16-02, 17-01, 18-01, and 18-02). In addition, we reviewed the directives and other relevant requirements as well as DHS's process for evaluating agency actions to address the requirements and to develop binding operational directive-related performance metrics. We also reviewed DHS's fiscal years 2018 and 2019 annual performance reports and quarterly performance report updates, fiscal year 2019 reports to OMB, and fiscal years 2016 and 2017 reports to Congress on agencies' (government-wide) implementation status of binding operational directives.

We assessed steps DHS was taking to measure agencies' performance against DHS's established metrics. Specifically, we reviewed the 99 civilian executive branch agencies' and 12 selected agencies' performance against the specific directives requirements. We analyzed agency documentation, including status reports and plans of action and milestones, as well as scanning data from the National Cybersecurity and Communications Integration Center for both selected agencies and government-wide. We also reviewed DHS performance reports regarding the extent to which DHS's government-wide performance metrics for mitigation of vulnerabilities on internet-facing systems and for closure of certain vulnerabilities on high value assets align with agencies' existing requirements from OMB and DHS, such as closure timelines of selected types of vulnerabilities and weaknesses. We compared these performance reports and metrics with existing requirements found in DHS's directives to assess whether they were aligned.

In addition, we reviewed detailed scanning data and output from a data analysis tool from DHS's database to determine the extent to which the 99 civilian executive branch agencies and our selected 12 agencies are

mitigating vulnerabilities on internet-accessible systems and whether or not they are being mitigated within given timeframes.[6]

In addition, to analyze the implementation of email and web security requirements, we reviewed detailed scanning data on the status of the 99 civilian executive branch agencies and our selected 12 agencies.[7] To assess the reliability of the scanning data and related DHS analysis that we used to support the findings in this report, we interviewed agency officials to determine the steps taken to ensure the integrity and reliability of the data and reviewed relevant documentation to substantiate the evidence obtained through interviews with agency officials. We determined that the data used in this report were sufficiently reliable for the purposes of our reporting objectives.

We supplemented our analyses with interviews of DHS and selected agency officials to obtain their views on the steps they have taken to address the directives' requirements.

We conducted this performance audit from October 2018 to February 2020 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[6]DHS, *Critical Vulnerability Mitigation Requirement for Federal Civilian Executive Branch Departments and Agencies' Internet-Accessible Systems,* BOD 15-01 (revoked and replaced by *Vulnerability Remediation Requirements for Internet-Accessible Systems,* BOD 19-02*),* issued May 21, 2015.

[7]DHS, *Enhance Email and Web Security*, BOD 18-01, October 16, 2017.

# Appendix II: List of Federal Agencies to Which Binding Operational Directives Apply

The Department of Homeland Security's (DHS) binding operational directives apply to all civilian executive branch agencies, but not to statutorily defined "national security systems," or certain systems operated by the Department of Defense or the intelligence community.[1] A list follows of the civilian executive branch agencies[2] that DHS tracks for compliance with the directives.[3]

1. Administrative Conference of the United States
2. Advisory Council on Historic Preservation
3. African Development Foundation Agency
4. American Battle Monuments Commission

[1]In this case, intelligence community is as defined by the *National Security Act of 1947,* as amended (50 U.S.C. § 3003(4)) and includes the following: Office of the Director of National Intelligence; the Central Intelligence Agency; the National Security Agency; the Defense Intelligence Agency; the National Geospatial-Intelligence Agency; the National Reconnaissance Office; other offices within the Department of Defense for the collection of specialized national intelligence through reconnaissance programs; the intelligence elements of the Army, the Navy, the Air Force, the Marine Corps, the Coast Guard, the Federal Bureau of Investigation, the Drug Enforcement Administration, and the Department of Energy; the Bureau of Intelligence and Research of the Department of State; the Office of Intelligence and Analysis of the Department of the Treasury; the Office of Intelligence and Analysis of the Department of Homeland Security, as well as other elements of any department or agency as may be designated by the President, or designated jointly by the Director of National Intelligence and the head of the department or agency concerned, as an element of the intelligence community.

[2]Although there are more than 99 federal civilian agencies, DHS's Cybersecurity and Infrastructure Security Agency (CISA) tracks the compliance of 99 federal civilian agencies with respect to the binding operational directives. CISA officials note that this list of agencies will change in fiscal year 2020. For a list of federal agencies, see the U.S. Government Manual 32 (2015).

[3]In addition to CISA's list of 99 agencies, the Christopher Columbus Fellowship Foundation was required to comply with the directives, but is not currently funded by Congress, according to its website. In addition, the Executive Office of the President is required to comply with the binding operational directives, but is not included in CISA's list.

5. Barry M Goldwater Scholarship Foundation
6. Broadcasting Board of Governors
7. Chemical Safety and Hazard Investigation Board
8. Commission of Fine Arts
9. Commodity Futures Trading Commission
10. Consumer Financial Protection Bureau
11. Consumer Product Safety Commission
12. Corporation for National and Community Service
13. Council of the Inspectors General on Integrity and Efficiency
14. Court Services and Offender Supervision Agency for the District of Columbia
15. Defense Nuclear Facilities Safety Board
16. Denali Commission
17. Department of Agriculture
18. Department of Commerce
19. Department of Education
20. Department of Energy
21. Department of Health and Human Services
22. Department of Homeland Security
23. Department of Housing and Urban Development
24. Department of Justice
25. Department of Labor
26. Department of State
27. Department of the Interior
28. Department of Transportation
29. Department of the Treasury
30. Department of Veterans Affairs
31. Election Assistance Commission
32. Environmental Protection Agency
33. Equal Employment Opportunity Commission

34. Export-Import Bank of the United States
35. Farm Credit Administration
36. Farm Credit System Insurance Corporation[4]
37. Federal Communications Commission
38. Federal Deposit Insurance Corporation
39. Federal Energy Regulatory Commission
40. Federal Financial Institutions Examination Council (including Federal Financial Institutions Examination Council Appraisal Subcommittee)
41. Federal Housing Finance Agency
42. Federal Labor Relations Authority
43. Federal Maritime Commission
44. Federal Mediation and Conciliation Service
45. Federal Mine Safety and Health Review Commission
46. Federal Reserve Board of Governors
47. Federal Retirement Thrift Investment Board
48. Federal Trade Commission
49. General Services Administration
50. Gulf Coast Ecosystem Restoration Council
51. Harry S. Truman Scholarship Foundation
52. Institute of Museum and Library Services
53. Inter-American Foundation
54. James Madison Memorial Fellowship Foundation
55. Marine Mammal Commission
56. Merit Systems Protection Board
57. Millennium Challenge Corporation
58. Morris K. Udall and Stewart L. Udall Foundation
59. National Aeronautics and Space Administration
60. National Archives and Records Administration

[4]Receives services and reports through the Farm Credit Administration.

61. National Capital Planning Commission
62. National Council on Disability
63. National Credit Union Administration
64. National Endowment for the Arts
65. National Endowment for the Humanities
66. National Labor Relations Board
67. National Mediation Board
68. National Science Foundation
69. National Transportation Safety Board
70. Nuclear Regulatory Commission
71. Nuclear Waste Technical Review Board
72. Occupational Safety and Health Review Commission
73. Office of Government Ethics
74. Office of Navajo and Hopi Indian Relocation
75. Office of Personnel Management
76. Office of Special Counsel
77. Overseas Private Investment Corporation
78. Peace Corps
79. Pension Benefit Guaranty Corporation
80. Postal Regulatory Commission
81. Presidio Trust
82. Privacy and Civil Liberties Oversight Board
83. Railroad Retirement Board
84. Securities and Exchange Commission
85. Selective Service System
86. Small Business Administration
87. Social Security Administration
88. Social Security Advisory Board
89. Surface Transportation Board
90. Tennessee Valley Authority

91. U.S. Trade and Development Agency
92. U.S. Agency for International Development
93. U.S. Section of International Boundary and Water Commission
94. United States AbilityOne Commission
95. United States Access Board
96. United States Commission on Civil Rights
97. United States Interagency Council on Homelessness
98. United States International Trade Commission
99. Vietnam Education Foundation

# Appendix III: Binding Operational Directives Process

Within the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency's Cybersecurity Division, the Federal Network Resilience (FNR) is responsible for managing the process for developing and overseeing the binding operational directives, including coordination and implementation. The process is documented in the department's draft *Cybersecurity Division Binding Operational Directives Process* and outlines five steps and their substeps:

**Step 1: Identify and Determine.** This step includes three substeps—**1.1 triggers, 1.2 business case development,** and **1.3 socialization**. The identification of a directive begins with a **trigger** that identifies a particular topic. The trigger may be from an administrative priority, technical assessment, operational finding, or discussions with external entities such as the Federal Chief Information Officer Council, National Institute of Standards and Technology (NIST), Office of Management and Budget (OMB) or a private sector organization. Once a topic is identified, FNR officials conduct research on the topic and solicit feedback from stakeholders.

FNR then directs topics to the Binding Operational Directives Discussion Group. According to the draft process, recommended members of this group include representatives from Cybersecurity and Infrastructure Security Agency (CISA) and ad hoc and external partners, such as OMB officials, federal CIOs and chief information security officers (CISO), NIST officials, and General Services Administration officials.

During substep 1.1, the group should decide whether to proceed to substep 1.2, **business case development** for a directives' topic. The group maintains an online repository for proposed topics, active directives, and topics that have been previously considered, but archived for future use or historical documentation purposes.

During business case development, a lead within the discussion group researches risks, threat actors, and mitigation strategies. The group

incorporates information from subject matter experts and programs that provide information on current threats facing agencies and mitigation actions (e.g., Continuous Diagnostics and Mitigation[1] and EINSTEIN).[2] Once drafted, the business case is sent to FNR leadership, such as the Director and Deputy Director, for review.

In the **socialization** substep 1.3, the discussion group may obtain additional feedback through various outreach efforts or through CIO, or CISO Council meetings.

**Step 2: Develop and Approve.** This step includes two substeps—**2.1 table top** and **2.2 BOD material finalization.** In step 2, FNR staff draft the directive. A **table top** exercise is an optional step that FNR staff may take to test required actions at selected agencies. As part of drafting the directive, the FNR staff coordinates with stakeholders, such as National Cybersecurity Assessments and Technical Services (NCATS), OMB and selected other agencies to develop an action plan template. This template instructs agencies on how to track and submit their progress on a particular directive. In addition, the team drafts a communications plan to disseminate directive-related information to agencies and the public. During substep 2.2, **BOD material finalization,** the action plan template and communications plan are sent along with the draft directive to all associated stakeholders (e.g. FNR, OMB, NIST, and Department of Homeland Security (DHS) Office of General Counsel) for review. After FNR staff incorporate any additional feedback, the draft directive package is then sent to the CISA Director for signature and then release.

**Step 3: Distribute.** This step includes three substeps—**3.1 notification, 3.2 baseline evaluation delivery,** and **3.3 begin mandatory actions.** According to FNR officials, the approval of a directive is the start of several processes in this step. During substep 3.1, all affected federal civilian agencies receive **notification** through an email and a directive issuance call within 24 hours of the signing of the directive. In addition,

[1]Continuous Diagnostics and Mitigation is a DHS program that provides cybersecurity tools, integration services, and dashboards to participating agencies to support them in improving their respective security posture.

[2]EINSTEIN is a DHS system that detects and blocks cyberattacks from compromising federal agencies and provides DHS with situational awareness to use threat information detected in one agency to protect the rest of the government and to help the private sector protect itself.

the DHS website (cyber.dhs.gov) and the OMB MAX portal may post the directive depending on the content of the directive.[3]

The notification of the directive is followed with agency **baseline evaluation delivery,** substep 3.2. As part of this substep, the validation team, including representatives from NCATS, may deliver baseline evaluations to provide agencies a better understanding of where they stand in addressing the directive prior to issuance, depending on the nature of the directive. In the last substep 3.3, agencies **begin mandatory actions** as noted in the directive.

**Step 4: Implement and Report.** This step includes three substeps—**4.1 action plan submission, 4.2 continuous coordination,** and **4.3 implementation and reporting.** The step begins with FNR's establishment of a Binding Operational Directives Implementation Team to manage the requirements of a specific directive. This team includes a technical lead who reviews and tracks **agency plan submissions** as part of substep 4.1; a validation team whose members validate agency compliance with the directive; and a data analyst, who is to compile all agency-submitted action plans and draft a monthly status report.

According to the draft process document, the validation team conducts directive-related scans and compliance checks, and develops and distributes scorecards that indicate agency compliance with directive requirements. For some directives, such as BODs 16-02, 17-01, and 18-02, DHS relied on agency self-reporting to confirm that an agency had addressed the requirements, and the validation team did not verify compliance. During substep 4.2 FNR staff and the affected agency maintain **continuous coordination** through email and phone conversations to address any challenges involved with implementing the directive. Substep 4.3 **implementation and reporting** consists of processes agencies may need to establish internally to address and report on directive requirements until completion, such as points of contact and methods of communication with FNR.

The implementation team produces monthly status reports for FNR leadership, such as the Director and Deputy Director, showing which agencies have complied or not complied with directive requirements.

[3]The Office of Management and Budget uses the MAX Information System to collect, validate, analyze, model, collaborate with agencies on, and publish information relating to its government-wide management and budgeting activities.

Based upon this information, FNR officials decide whether to escalate instances of agency noncompliance.[4] In addition, FNR officials stated that they have a monthly check-in with OMB, during which they provide status reports as well as conduct less formal weekly discussions. For Congress, CISA produces an annual binding operational directives' implementation report, in addition to responding to more frequent congressional information requests. To date, DHS has submitted two congressional reports for fiscal year 2016 and 2017. According to FNR officials, as of September 2019, the fiscal year 2018 report is undergoing OMB review.

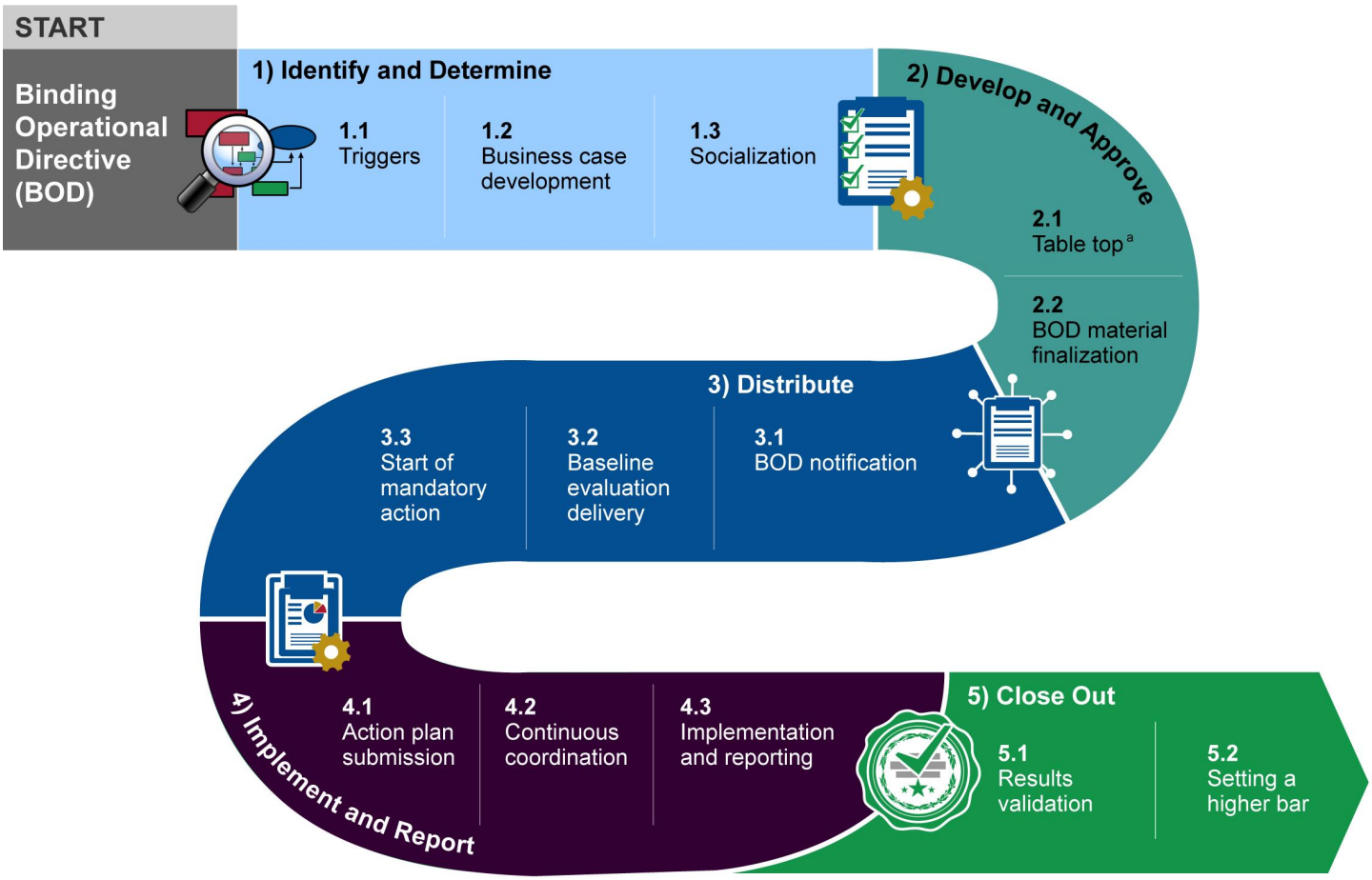
**Step 5: Close Out.** This step includes two substeps—**5.1 results validation** and **5.2 setting a higher bar.** The draft process document describes the following scenarios that may lead to **results validation;** if a directive: (1) has been completed by all agencies; (2) is no longer necessary because it has been revoked, suspended, or codified into law; or (3) needs to be amended. In the first scenario, once the validation team affirms that the requirements have been met, FNR officials are to notify affected federal agency officials that their agencies have fulfilled all requirements. FNR officials then draft a binding operational directive completion letter that the Secretary of DHS or the Secretary's designee signs.[5] According to FNR officials, a directive does not fully close out after the Secretary signs a completion letter, because the directive is still in effect even after agencies have fulfilled all of the particular directive's requirements. If a directive is revoked or amended, FNR officials draft a letter noting the reasons for such actions which the Secretary of DHS then signs. Agencies are expected to adhere to the newly implemented requirement, which is how DHS describes substep 5.2, **setting a higher bar.**

Figure 1 provides the life cycle of a binding operational directive.

[4]According to DHS, the escalation process brings nonadherence by an agency to the attention of that agency's senior officials. They are charged with resolution of the issue, thereby ensuring that their agencies adhere to the cybersecurity requirements, directives, and mandates. According to DHS officials, since the issuance of Binding Operational Directive 15-01, there have been 22 escalations to the agency chief information officer level or higher.

[5]BOD 16-02, *Threat to Network Infrastructure Devices*, and BOD 17-01, *Removal of Kaspersky-branded Products* were completed on November 6, 2018 and July 27, 2018, respectively.

**Figure 5: Department of Homeland Security Binding Operational Directive Life Cycle**




Source: GAO analysis of Department of Homeland Security data. | GAO-20-133

Note: "Table top" is a dry run of the draft directive, during which one or more agencies test the scope, scale, and requirements being proposed.

# Appendix IV: Binding Operational Directives and Associated Requirements

The Department of Homeland (DHS) had issued eight binding operational directives (BOD) as of October 2019. A full list of DHS's directives' numbers and titles with a summary of their corresponding DHS and agency requirements follows.

## BOD 15-01– **Critical Vulnerability Mitigation Requirement for Federal Civilian Executive Branch Departments and Agencies' Internet-Accessible Systems,** May 21, 2015[1]

### Agency Requirements

Agencies or departments are to:

- Review and mitigate the critical vulnerabilities on their internet facing systems identified by DHS's National Cybersecurity and Communications Integration Center within 30 days of issuance of agencies' weekly cyber hygiene reports.
- Within 30 days will provide a detailed justification to DHS outlining any barriers, planned steps for resolution, and a time frame for mitigation, if unable to mitigate vulnerability.

### DHS Requirements

- DHS's Federal Network Resilience Division will work directly with the department or agency to attempt to assist or address any constraints limiting expedited resolution of the vulnerability.

[1]https://cyber.dhs.gov/bod/15-01/BOD 15-01 has been revoked and replaced by BOD 19-02 *Vulnerability Remediation Requirements for Internet-Accessible Systems*.

- DHS's NCCIC will leverage weekly agency scans to track each department or agency's progress in mitigating its critical vulnerabilities.
- DHS will provide quarterly cyber hygiene report updates to the OMB to ensure department and agency results are synchronized with OMB cybersecurity oversight initiatives.

## BOD 16-01–**Securing High Value Assets,** June 9, 2016[2]

### Agency Requirements

Agencies or departments are to:

- Identify and submit the name of a lead point of contact to DHS's FNR branch within 7 days of this directive's issuance. The point of contact will be responsible for coordinating the agency's high value asset assessments with DHS. (Submission of the same information for at least one backup point of contact is encouraged.)
- Participate in assessments, mitigation, and remediation activities by:
- Signing a DHS-provided rules of engagement document authorizing DHS to conduct risk and vulnerability assessments on agency high value assets.
- Beginning to implement DHS-issued mitigation measures listed in this directive's appendix for agency high value assets
- Participating in the high value asset assessments authorized by the rules of engagement.
- Participating in a security architecture assessment for select high value assets, if requested to do so by DHS.
- Mitigating the high-priority vulnerabilities identified by DHS in the high value asset final assessment report within 30 days of DHS's receipt of the report or determine that mitigation is not feasible within that time frame.
- Providing additional status updates every 30 days until all high-priority vulnerabilities have been addressed.

### DHS Requirements

- DHS will identify agency high value assets for assessment and report their findings to agencies.
- DHS will validate whether any relevant protections have been appropriately implemented during each high value asset assessment and

[2]https://cyber.dhs.gov/bod/16-01/. BOD 16-01 has been revoked and replaced by BOD 18-02 *Securing High Value Assets*.

will provide the agency with a report on the extent of sufficient implementation.

- If an agency does not comply with the requirements of this binding operational directive, DHS will follow up with each deputy secretary or equivalent, as appropriate.

## BOD 16-02–**Threat to Network Infrastructure Devices,** September 27, 2016[3]

### Agency Requirements

Agencies or departments are to:

- Perform all actions in the Solution sections of the technical annexes to the NCCIC Analysis Report AR-16-20173[4] no later than 45 days after issuance of this directive.
- Report to DHS, through the OMB MAX Connect Portal, either full mitigation or provide a detailed plan of action and milestones explaining the constraints preventing mitigation and the associated compensating controls established no later than 45 days after issuance of this directive.
- Provide additional reports or plans of action and milestones every 30 days thereafter until full mitigation is achieved.

### DHS Requirements

- DHS's NCCIC will continue to analyze information for additional mitigation steps to protect federal networks and will develop technical annexes in the future under this directive as necessary.

[3]https://cyber.dhs.gov/bod/16-02/

[4]DHS's NCCIC published an analysis report (AR)-16-2017 *The Increasing Threat to Network Infrastructure Devices and Recommended Mitigations,* (AR)-16-2017 (Washington, D.C.: August 30, 2016) (https://cyber.dhs.gov/assets/report/ar-16-20173.pdf) to inform security professionals and network administrators at government departments or agencies of potential threats to network infrastructure devices, especially routers and firewalls. The report also offers solutions to mitigate these vulnerabilities in three technical annexes.

- If an agency does not comply with the requirements of this directive, DHS will follow up with each deputy secretary or equivalent, as appropriate.
- Perform all actions in the Solution sections of the technical annexes to the NCCIC Analysis Report AR-16-20173[5] no later than 45 days after issuance of this directive.
- Report to DHS, through the OMB MAX Connect Portal, either full mitigation or provide a detailed plan of action and milestones explaining the constraints preventing mitigation and the associated compensating controls established no later than 45 days after issuance of this directive.
- Provide additional reports or plans of action and milestones every 30 days thereafter until full mitigation is achieved.

## BOD 16-03–**2016 Agency Cybersecurity Reporting Requirements,** October 17, 2016[6]

### Agency Requirements

Agencies or departments are to:

- Report security incidents to the DHS United States Computer Emergency Readiness Team in accordance with the guidelines found at https://www.us-cert.gov/incident-notification-guidelines, which are updated as necessary.
- Include metric information from the chief information officer, inspector general, and senior agency official for privacy, detailed in the annual FISMA metrics, in the Fiscal Year 2016 Annual Federal Information Security Management Act Reports, found at https://www.dhs.gov/publication/fy16-fisma-documents.

[5]DHS's NCCIC published an analysis report (AR)-16-2017 *The Increasing Threat to Network Infrastructure Devices and Recommended Mitigations,* (AR)-16-2017 (Washington, D.C.: August 30, 2016) (https://cyber.dhs.gov/assets/report/ar-16-20173.pdf) to inform security professionals and network administrators at government departments or agencies of potential threats to network infrastructure devices, especially routers and firewalls. The report also offers solutions to mitigate these vulnerabilities in three technical annexes.

[6]https://cyber.dhs.gov/bod/16-03/

- Submit CIO, IG, and privacy metrics by November 10, 2016, to OMB and DHS via CyberScope.
- View the Fiscal Year 2017 Annual FISMA CIO metrics available at https://www.dhs.gov/publication/fy17-fisma-documents and plan accordingly so they can include these metrics in their Fiscal Year 2017 FISMA Reports.

DHS Requirements

DHS will track submission of Fiscal Year 2016 Annual Federal Information Security Management Act Reports and privacy metrics, and follow up with OMB or the relevant agency to address non-compliance as appropriate.

## BOD 17-01–**Removal of Kaspersky-branded Products,** September 13, 2017[7]

Agency Requirements

Agencies or departments are to:

- Within 30 calendar days after issuance of this directive, identify the use or presence of Kaspersky-branded products on all federal information systems and provide a report to DHS that includes:
- A list of Kaspersky-branded products found on agency information systems. If agencies do not find the use or presence of Kaspersky-branded products on their federal information systems, they should inform DHS that no Kaspersky- branded products were found.
- The number of endpoints impacted by each product.
- The methodologies employed to identify the use or presence of the products.
- Within 60 calendar days after issuance of this directive, develop and provide to DHS a detailed plan of action to remove and discontinue present and future use of all Kaspersky-branded products beginning 90 calendar days after issuance of this directive. Agency plans must address the following elements:

[7]https://cyber.dhs.gov/bod/17-01

- Agency name.
- Point of contact information, including name, telephone number, and email address.
- List of identified products.
- Number of endpoints impacted.
- Methodologies employed to identify the use or presence of the products.
- List of agencies (components) impacted within department.
- Mission function of impacted endpoints and/or systems.
- All contracts, service-level agreements, or other agreements the agency has entered into with Kaspersky.
- Timeline to remove identified products.
- If applicable, FISMA performance requirements or security controls that product removal would impact, including, but not limited to data loss/ leakage prevention, network access control, mobile device management, sandboxing/detonation chamber, web site reputation filtering/web content filtering, hardware and software whitelisting, vulnerability and patch management, anti-malware, anti-exploit, spam filtering, data encryption, or other capabilities.
- If applicable, chosen or proposed replacement products/capabilities.
- If applicable, timeline for implementing replacement products/ capabilities.
- Foreseeable challenges not otherwise addressed in this plan.
- Associated costs related to licenses, maintenance, and replacement (coordinate with agency chief financial officers).
- At 90 calendar days after issuance of this directive, and unless directed otherwise by DHS based on new information, departments or agencies will begin to implement the agency plan of action and provide a status report to DHS on the progress of that implementation every 30 calendar days thereafter until full removal and discontinuance of use is achieved.

DHS Requirements

- DHS will rely on agency self-reporting and independent validation measures for tracking and verifying progress.
- DHS will provide additional guidance through the federal cybersecurity coordination, assessment, and response protocol following the issuance of this directive.

## BOD 18-01– **Enhance Email and Web Security,** October 16, 2017[8]

### Agency Requirements

Agencies or departments are to:

- Within 30 calendar days after issuance of this directive, develop and provide to DHS an agency plan of action for BOD 18-01 to:
- Enhance email security by configuring within 90 days after issuance of this directive:
- All internet-facing mail servers to offer STARTTLS, and
- All second-level agency domains to have valid sender policy framework (SPF)/domain-based message authentication, reporting and conformance (DMARC) records, with at minimum a DMARC policy of “p=none” and at least one address defined as a recipient of aggregate and/or failure reports.
- Within 120 days after issuance of this directive, ensuring:
- Secure sockets layer (SSL)v2 and SSLv3 are disabled on mail servers, and
- Triple data encryption standard (3DES) and Rivest cipher 4 (RC4) ciphers are disabled on mail servers (see temporary policy exception for 3DES).
- Within 15 days of the establishment of centralized NCCIC reporting location, adding the NCCIC as a recipient of DMARC aggregate reports.
- Within 1 year after issuance of this directive, setting a DMARC policy of “reject” for all second-level domains and mail-sending hosts.
- Enhance web security by:
- Within 120 days after issuance of this directive, ensuring:
- All publicly accessible federal websites and web services provide service through a secure connection (hypertext transfer protocol secure (HTTPS)-only, with HTTP strict transport security (HSTS)),

[8]https://cyber.dhs.gov/bod/18-01/

- SSLv2 and SSLv3 are disabled on web servers, and
- 3DES and RC4 ciphers are disabled on web servers.
- Identifying and providing a list to DHS of agency second-level domains that can be HSTS preloaded, for which HTTPS will be enforced for all subdomains.
- Upon delivery of its plans of action for BOD 18-01, within 30 days of this directive, departments or agencies will begin implementing their plans.
- At 60 calendar days after issuance of this directive, departments or agencies will provide a report to DHS on the status of that implementation. They will continue to report every 30 calendar days thereafter until implementation of the agency's BOD 18-01 plan is complete.

### DHS Requirements

- DHS will review each agency plan of action for BOD 18-01 after receipt and may contact agencies with concerns.
- DHS will coordinate the agency-provided lists of domains for HSTS preloading with DotGov.
- DHS will rely on scanning by its National Cybersecurity Assessments and Technical Services team for tracking and verifying progress with agency compliance with this directive.
- DHS will notify agencies when the NCCIC establishes a central location for the collection of agency DMARC aggregate reports
- DHS will provide additional guidance through a DHS coordination call and other engagements and products following the issuance of this directive.

## BOD 18-02– **Securing High Value Assets,** May 7, 2018[9]

### Agency Requirements

Agencies or departments are to:

[9]https://cyber.dhs.gov/bod/18-02/

- Identify and submit coordination points of contact (POC) for high value asset assessments.
- Identify a lead, federal employee POC and at least one backup federal employee POC responsible for coordinating the agency HVA assessments with DHS.1
- Submit within 7 days of the issuance of this directive, the following contact information to a specified DHS email address for the agency's lead POC and backup POC:
- Name
- Position/title
- Email addresses: Unclassified and, if available, classified accounts
- Phone number
- Review, at least annually, agency POC information, and re-certify or submit updates as changes are made.
- Submit agency high value assets.
- Submit a current and prioritized HVA list for all agency/ department components within 30 days of issuance of this directive, using the identified HVA POC homeland security information network (HSIN) account.
- Once submitted, review the HVA lists on a quarterly basis and provide updates and modifications via HSIN.
- Participate in an annual meeting, coordinated by DHS, to validate the agency HVA lists.
- Participate in DHS-led assessments
- If selected to participate in DHS-led HVA assessment, departments or agencies will complete and submit to DHS a single rules of engagement (ROE), and for each HVA and related system(s) to be assessed, one ROE Appendix A titled "Risk and Vulnerability Assessment (RVA) Services for High Value Assets and Related Systems," authorizing DHS to conduct HVA RVAs on that agency HVA and related systems.
- Participate in the HVA assessments authorized by the ROE and one or more Appendix A submissions for "RVA Services for High Value Assets and Related Systems."

- Participate in a security architecture review (SAR) of each HVA to be assessed.
- Impose no restrictions on the timing and/or frequency of the assessments, the services to be provided by DHS, or the scope of systems that are part of or related to the HVA being assessed.
- Ensure timely remediation of identified vulnerabilities and report mitigation plans and progress
- Within 30 days of receipt of the RVA and/or SAR reports identifying major or critical weakness to an assessed HVA, remediate all major or critical weaknesses and provide notification to DHS that each identified weakness was addressed.
- If it is determined by the designated senior accountable official for risk management that full remediation cannot be completed within the initial 30-day time frame, develop and submit to a designated DHS email address, a remediation plan for each HVA with remaining major or critical weaknesses within 30 days of the receipt of the RVA and/or SAR reports.
- This remediation plan shall include justification for the extended timeline, the proposed timeline and associated milestones to remediation (not to exceed 1 year), interim mitigation actions planned to address immediate vulnerabilities, and, if relevant, the identification of constraints related to policy, budget, workforce, and operations.
- This remediation plan must be signed by the designated senior accountable official for risk management prior to submission to DHS.
- Report the status of each remaining major or critical weakness to a designated DHS email address every 30 days until full remediation is achieved for all assessed HVAs. Status reports must address RVA and SAR results through combined reporting and must be submitted every 30 days starting 30 days after the submission of the remediation plan described above.
- Notify DHS at a designated email address and through the monthly status reports of any modifications to remediation plan timelines and when full remediation has been achieved. The notifications for modifications and full remediation must be certified under signature of the designated senior accountable official for risk management.

## DHS Requirements

- DHS will centrally manage agency progress and report submissions, and will engage each agency head in all cases where the agency has not met the deadlines outlined in the agency/department required actions list.
- DHS collects, maintains, and prioritizes agency-submitted HVAs, and will notify enterprise chief information officers, chief information security officers, and HVA points of contact of specific HVAs selected for DHS-led assessments based on OMB-led determinations.
- DHS maintains all agency HVA submissions on HSIN. DHS provisions HSIN accounts for designated agency HVA POCs and provides instruction on HSIN use, as needed.
- DHS provides standard templates for identifying and submitting agency HVAs and for remediation plans and progress reports.
- DHS plans and conducts RVAs and SARs for OMB-selected agency HVAs, and provides formal reports containing assessment findings and recommendations to the designated agency HVA POCs.

## BOD 19-02– **Vulnerability Remediation Requirements for Internet Accessible Systems,** April 29, 2019[10]

### Agency Requirements

Agencies or departments are to:

- Ensure access and verify scope.
- Ensure cyber hygiene scanning access by removing cyber hygiene source internet protocol (IP) addresses from block lists.
- Within 5 working days of the change, notify the Cybersecurity and Infrastructure Security Agency (CISA) at a designated email address of any modifications to the agency's internet-accessible IP addresses. This includes newly acquired internet-accessible IP addresses or re-assigned internet-accessible IP addresses that are no longer part of the agency's asset inventory.
- Upon request from CISA, departments or agencies will submit updated cyber hygiene agreements to a designated DHS email address.
- Review and remediate critical and high vulnerabilities.
- Review cyber hygiene reports issued by CISA and remediate the critical and high vulnerabilities detected on the agency's internet-accessible systems as follows:
- Critical vulnerabilities must be remediated within 15 calendar days of initial detection.
- High vulnerabilities must be remediated within 30 calendar days of initial detection.
- If vulnerabilities are not remediated within the specified time frames, CISA will send a partially populated remediation plan identifying all overdue, in-scope vulnerabilities to the agency point of contact for validation and population. Departments or agencies shall return the completed remediation plan within 3 working days of receipt to a designated FNR email address. The recipient of the remediation plan shall complete the following fields in the remediation plan:

[10]https://cyber.dhs.gov/bod/19-02/

- Vulnerability remediation constraints
- Interim mitigation actions to overcome constraints
- Estimated completion date to remediate the vulnerability

DHS Requirements

- CISA will monitor federal agency progress and will engage agency senior leadership, such as the chief information security officer, the chief information officer, and the senior accountable officer for risk management, as necessary and appropriate, when the agency has not met the required agency action deadlines specified.
- CISA also will track the remediation of critical and high vulnerabilities through persistent cyber hygiene scanning and will validate compliance with the directive requirements through these reports.
- CISA will provide regular reports to federal civilian agencies on cyber hygiene scanning results and current status, and a federal enterprise scorecard report to agency leadership.
- CISA will provide standard remediation plan templates for federal civilian agencies to populate if remediation efforts exceed required time frames.
- CISA will engage agency POCs to discuss agency status and provide technical expertise and guidance for the remediation of specific vulnerabilities, as requested and appropriate.
- CISA will engage agency chief information security officer, the chief information officer, and the senior accountable officer for risk management, throughout the escalation process, if necessary.
- CISA will provide monthly cyber hygiene reports to OMB to identify cross-agency trends, persistent challenges, and facilitate potential policy and/or budget-related actions and remedies. The report will also ensure alignment with other OMB-led cybersecurity oversight initiative.

# Appendix V: Technical Requirements Explanation for *Enhance Email and Web Security,* Binding Operational Directive 18-01

The scope of Binding Operational Directive (BOD) 18-01, *Enhance Email and Web Security,* includes complex technical concepts that require background knowledge on various topics for both email and web security. The following information provides more detail on the directive's technical requirements.[1]

## Email Security

### STARTLS

When enabled by a receiving mail server, **STARTTL**S signals to a sending mail server that the capability to encrypt an email in transit is present. While it does not force the use of encryption, enabling STARTTLS makes passive man-in-the-middle attacks more difficult.

### Email Authentication

**SPF** (Sender Policy Framework) and **DKIM** (Domain Keys Identified Mail) allow a sending domain to effectively "watermark" its emails, making unauthorized emails (e.g., spam, phishing email) easy to detect. When an email is received that does not pass an agency's posted SPF/DKIM rules, **DMARC** (Domain-based Message Authentication, Reporting & Conformance) tells a recipient what the domain owner would like done with the message.

[1]The directive is available in full at https://cyber.dhs.gov/bod/18-01/

Setting a DMARC policy of “reject” provides the strongest protection against spoofed email, ensuring that unauthenticated messages are rejected at the mail server, even before delivery. Additionally, DMARC reports provide a mechanism for an agency to be made aware of the source of an apparent forgery, information that they would not normally receive otherwise. Multiple recipients can be defined for the receipt of DMARC reports.

### Web Security

**Hypertext Transfer Protocol (HTTP)** connections can be easily monitored, modified, and impersonated; **Hypertext Transfer Protocol Secure (HTTPS)** remedies these vulnerabilities. **HTTP Strict Transport Security (HSTS)** ensures that browsers always use an https:// connection, and removes the ability for users to click through certificate-related warnings. In 2015, OMB M-15-13, *Policy to Require Secure Connections Across Federal Websites and Web Services,* required all existing federal websites and web services to be accessible through a secure connection (HTTPS-only, with HSTS). In 2017, the .gov registry began automatically preloading new federal .gov domains as HSTS-only in modern browsers.

### Protocols

**SSL** (secure sockets layer) is a computing protocol that ensures the security of data sent via the internet by using encryption. SSLv2 was released in 1995. Most modern clients do not support SSLv2, but a cross-protocol security bug (DROWN) demonstrated that merely serving SSLv2 enables the inspection of traffic encrypted with the more modern and secure protocol, transport layer security.

SSLv3 was released in 1996 and considered to be insecure after a man-in-the-middle exploit (POODLE) was published in 2014.

### Ciphers

**RC4** (Rivest Cipher 4) is a stream cipher algorithm that is used in popular protocols such as SSL (to protect internet traffic) and wired equivalent privacy (WEP) to secure wireless networks. In 2014, NIST marked RC4 as “not approved” for use in federal information systems.

**3DES** (3 key triple data encryption standard) is an implementation of the data encryption standard (DES) algorithm that uses three passes of the

DES algorithm instead of one as used in ordinary DES applications. Triple DES provides much stronger encryption than ordinary DES, but it is less secure than advanced encryption standard. In 2017, NIST urged all users of 3DES to migrate as soon as possible.

# Appendix VI: Comments from the Department of Homeland Security

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

January 15, 2020

Vijay A. D'Souza
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Management Response to Draft Report GAO-20-133, "INFORMATION TECHNOLOGY: DHS Directives Have Strengthened Federal Cybersecurity, but Improvements Are Needed"

Dear Mr. D'Souza:

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

The Department is pleased to note GAO's positive recognition of efforts, primarily led by DHS's Cybersecurity and Infrastructure Security Agency (CISA), to mitigate and address critical vulnerabilities within the federal cyber space through our Binding Operational Directives (BODs). The Department's ability to issue directives, support and oversee implementation, and assess and validate the results is a critical element of our work, and allows DHS to strengthen federal cybersecurity through close coordination with our stakeholders and agency partners. It is important to note that during this review, DHS was in the process of updating the cybersecurity directives process to incorporate several key lessons learned and enhancement opportunities identified over the past several years. As threats evolve and BODs continue to be implemented across agencies, DHS remains committed to strengthening its management processes, procedures, and technical capabilities to better address enterprise risks and emerging threats through the directives process.

The draft report contained four recommendations, with which the Department concurs. Attached find our detailed response to each recommendation. DHS previously submitted technical comments under a separate cover.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Sincerely,

JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Attachment

2

## Attachment: Management Response to Recommendations Contained in GAO-20-133

GAO recommended that the Secretary of Homeland Security:

**Recommendation 1:** Determine when in the directive development process—for example, during early development and at directive approval—coordination with relevant stakeholders, including NIST [National Institute of Standards and Technology] and GSA [General Services Administration], should occur.

**Response:** Concur. DHS recognizes the importance of coordinating with relevant stakeholders such as NIST and GSA. In fact, CISA's Cybersecurity Division's (CSD) engagement on directive coordination included NIST, GSA, and the Office of Management and Budget (OMB). In addition, CISA coordinated with the Department of Defense and the Federal cyber leadership councils during the past year to align efforts, and share insights and perspectives. Through this collaboration, CSD identified the need to establish and leverage a federal cybersecurity community of interest to refine and strengthen certain DHS directives and coordinated actions. CSD is currently in the process of revising the directive development process. Once updated, the process documentation will further clarify when, how, with whom, and under which circumstances DHS coordinates with key partners during the development process. Estimated Completion Date (ECD): September 30, 2020.

**Recommendation 2:** Develop a strategy to independently validate selected agencies' self-reported actions on meeting binding operational directive requirements, where feasible, using a risk-based approach.

**Response:** Concur. Due to the nature of the BOD authority and the fact that requirements specified within a directive could cover a wide range of topics, issues, and risks, CSD must consider validation methods early in the development process to help frame eventual implementation. Though automated validation mechanisms such as ongoing scanning and continuous monitoring are preferred, CSD believes that the urgency to act on specific threats and enterprise risks to the federal information technology (IT) enterprise should never be slowed or scoped down just to ensure that results can be validated by automated means. Even when an optimal validation mechanism is not available, directives can remain the most effective means to prioritize and coordinate agency actions, specify requirements and timeframes, and set clear expectations for agency cyber leadership when determining agency-level risk management approaches.

Though DHS' continuous engagement with agency cyber leadership on the content of agency self-reported information increases confidence in the results, CSD is actively

3

working to advance technical capabilities to enable independent validation, while also refining and focusing management processes to enable further risk-based review and verification of BOD status at individual agencies. It is in this spirit that CSD is currently working to formalize a risk-based strategy to validate agency results. CSD is confident that full deployment and integration of Continuous Diagnostics and Mitigation CDM program capabilities will significantly increase our ability to validate results similar to our current use of cyber hygiene scans. Furthermore, CSD is working with OMB to restructure and focus the CyberStat review process to address the need for independent validation. CSD intends for this type of management review to not only validate agency-submitted results, but to also help identify support opportunities and specific actions to address agency progress, challenges, and constraints related to BOD implementation. ECD: September 30, 2020.

**Recommendation 3:** Ensure that the binding operational directive performance metric for addressing vulnerabilities identified by high value asset assessments aligns with the process DHS has established.

**Response:** Concur. DHS recognizes the importance of ensuring processes are aligned to drive efficiency and enhance coordination with relevant stakeholders. As such, CSD will continue to evaluate High Value Asset (HVA) Plans of Action and Milestone and appropriate BOD performance metrics to ensure they conform to established and approved processes. CSD will also conduct an analysis in order to update the process and metrics to ensure future alignment. ECD: April 30, 2020.

**Recommendation 4**: Develop a schedule and plan for completing the high value asset program reassessment and addressing the outstanding issues on completing the required high value asset assessments, identifying needed resources, and finalizing guidance for Tier 2 and 3 HVA systems.

**Response:** Concur. CSD's schedule for completing HVA reassessments will continue to repreform Risk and Vulnerability Assessments (RVAs) and Security Architecture Reviews (SARs) every three years. DHS' CISA continues to onboard additional assessment staff, streamline processes, and pursue other continuous improvement efforts to ensure that the agency can perform RVAs and SARs at the necessary rate to perform all 212 Tier 1 assessments every 36 months.

CSD is currently conducting a pilot Cyber Qualification Initiative (CQI), which provides a system for non-CISA teams to perform assessment services to the same level of quality as CISA. Once the CQI is out of the pilot phase and is offered to agency teams and third-party assessors (projected Q4 2020), it will become a major element of the guidance provided to agencies regarding Tier 2 and Tier 3 HVAs. ECD: September 30, 2020.

4

## GAO Contact

# Appendix VII: GAO Contact and Staff Acknowledgments

Vijay A. D'Souza at 202-512-6240 or dsouzav@gao.gov

## Staff Acknowledgments

In addition to the contact named above, Neelaxi Lakhmani (assistant director), Kathleen S. Epperson (analyst-in-charge), Season Burris, Christopher Businsky, Noah Levesque, David Matcham, T. Bruce Rackliff, Karl Seifert, and Priscilla Smith made key contributions to the report.

# Appendix VIII: Accessible Data

## Data Tables

**Figure 1: Department of Homeland Security Binding Operational Directive (BOD), Percent of Critical Vulnerabilities Mitigated within 30 days, Government-wide and 12 Selected Agencies, May 21, 2015 through May 20, 2019**

| Category | Government-wide | 12 Agencies |
|---|---|---|
| 5/21/15 through 5/20/16 (1st year with BOD 15-01) | 57.6 | 60.8 |
| 5/21/16 through 5/20/17 (2nd year with BOD 15-01) | 86.7 | 89.5 |
| 5/21/17 through 5/20/18 (3rd year with BOD 15-01) | 84.7 | 81.4 |
| 5/21/18 through 5/20/19 (4th year with BOD 15-01, to date)a | 61.2 | 65.9 |

**Figure 2: Federal Civilian Agency Progress in Mitigating Vulnerable Network Infrastructure Devices, September 2016 through January 2019**

| Mitigation time frame | Number of network infrastructure devices |
|---|---|
| Q1 | 11474 |
| Q2 | 6080 |
| Q3 | 3176 |
| Q4 | 1093 |
| Q1 | 555 |
| Q2 | 528 |
| Q3 | 426 |
| Q4 | 162 |
| Q1 | 9 |
| Q2 | 0 |

**Figure 3: Department of Homeland Security Binding Operational Directive (BOD) 18-01 Government-wide Implementation across Domains by Directive Requirement, as of May 13, 2019**

| Directive requirements | Percent of email domains and web hosts in compliance |
|---|---|
| STARTTLS supported | 99 |
| Valid DMARC record | 99 |
| DHS received DMARC | 99 |
| DMARC “p-reject” implemented | 92 |
| HTTPS enforced | 90 |
| Strong HSTS used | 86 |
| Weak email protocols and ciphers disabled | 83 |
| Weak web protocols and ciphers disabled | 98 |

**Figure 4: Compliance with Department of Homeland Security Binding Operational Directive 18-01 Email and Web Security Requirements in March 2018, October 2018, and May 2019**

| Date | Gov-wide | Agency |
|---|---|---|
| Mar 26, 2018 | 4 | 8 |
| Oct 17, 2018 | 7 | 17 |
| May 13, 2019 | 7 | 25 |

# Agency Comment Letter

## Accessible Text for Appendix VI Comments from the Department of Homeland Security

### Page 1

January 15, 2020

Vijay A. D’Souza

Director, Information Technology and Cybersecurity

U.S. Government Accountability Office

441 G Street, NW

Washington, DC 20548

Re: Management Response to Draft Report GAO-20-133, "INFORMATION TECHNOLOGY: DHS Directives Have Strengthened Federal Cybersecurity, but Improvements Are Needed"

Dear Mr. D'Souza:

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

The Department is pleased to note GAO's positive recognition of efforts, primarily led by DHS's Cybersecurity and Infrastructure Security Agency (CISA), to mitigate and address critical vulnerabilities within the federal cyber space through our Binding Operational Directives (BODs). The Department's ability to issue directives, support and oversee implementation, and assess and validate the results is a critical element of our work, and allows DHS to strengthen federal cybersecurity through close coordination with our stakeholders and agency partners. It is important to note that during this review, DHS was in the process of updating the cybersecurity directives process to incorporate several key lessons learned and enhancement opportunities identified over the past several years. As threats evolve and BODs continue to be implemented across agencies, DHS remains committed to strengthening its management processes, procedures, and technical capabilities to better address enterprise risks and emerging threats through the directives process.

The draft report contained four recommendations, with which the Department concurs. Attached find our detailed response to each recommendation. DHS previously submitted technical comments under a separate cover.

Page 2

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Sincerely,

JIM H. CRUMPACKER, CIA, CFE

Director

Departmental GAO-OIG Liaison Office

Attachment

Page 3

Attachment: Management Response to Recommendations

Contained in GAO-20-133

GAO recommended that the Secretary of Homeland Security:

Recommendation 1: Determine when in the directive development process-for example, during early development and at directive approval-coordination with relevant stakeholders, including NIST [National Institute of Standards and Technology] and GSA [General Services Administration], should occur.

Response: Concur. DHS recognizes the importance of coordinating with relevant stakeholders such as NIST and GSA. In fact, CISA's Cybersecurity Division's (CSD) engagement on directive coordination included NIST, GSA, and the Office of Management and Budget (0MB). In addition, CISA coordinated with the Department of Defense and the Federal cyber leadership councils during the past year to align efforts, and share insights and perspectives. Through this collaboration, CSD identified the need to establish and leverage a federal cybersecurity community of interest to refine and strengthen certain DHS directives and coordinated actions. CSD is currently in the process of revising the directive development process. Once updated, the process documentation will further clarify when, how, with whom, and under which circumstances DHS coordinates with key partners during the

development process. Estimated Completion Date (ECD): September 30, 2020.

Recommendation 2: Develop a strategy to independently validate selected agencies' self-reported actions on meeting binding operational directive requirements, where feasible, using a risk-based approach.

Response: Concur. Due to the nature of the BOD authority and the fact that requirements specified within a directive could cover a wide range of topics, issues, and risks, CSD must consider validation methods early in the development process to help frame eventual implementation. Though automated validation mechanisms such as ongoing scanning and continuous monitoring are preferred, CSD believes that the urgency to act on specific threats and enterprise risks to the federal information technology (IT) enterprise should never be slowed or scoped down just to ensure that results can be validated by automated means. Even when an optimal validation mechanism is not available, directives can remain the most effective means to prioritize and coordinate agency actions, specify requirements and timeframes, and set clear expectations for agency cyber leadership when determining agency-level risk management approaches.

Though DHS' continuous engagement with agency cyber leadership on the content of agency self-reported information increases confidence in the results, CSD is actively

Page 4

working to advance technical capabilities to enable independent validation, while also refining and focusing management processes to enable further risk-based review and verification of BOD status at individual agencies. It is in this spirit that CSD is currently working to formalize a risk-based strategy to validate agency results. CSD is confident that full deployment and integration of Continuous Diagnostics and Mitigation CDM program capabilities will significantly increase our ability to validate results similar to our current use of cyber hygiene scans. Furthermore, CSD is working with 0MB to restructure and focus the CyberStat review process to address the need for independent validation. CSD intends for this type of management review to not only validate agency- submitted results, but to also help identify support opportunities and specific actions to address agency progress, challenges, and constraints related to BOD implementation. ECD: September 30, 2020.

Recommendation 3: Ensure that the binding operational directive performance metric for addressing vulnerabilities identified by high value asset assessments aligns with the process DHS has established.

Response: Concur. DHS recognizes the importance of ensuring processes are aligned to drive efficiency and enhance coordination with relevant stakeholders. As such, CSD will continue to evaluate High Value Asset (HVA) Plans of Action and Milestone and appropriate BOD performance metrics to ensure they conform to established and approved processes. CSD will also conduct an analysis in order to update the process and metrics to ensure future alignment. ECD: April 30, 2020.

Recommendation 4: Develop a schedule and plan for completing the high value asset program reassessment and addressing the outstanding issues on completing the required high value asset assessments, identifying needed resources, and finalizing guidance for Tier 2 and 3 HYA systems.

Response: Concur. CSD's schedule for completing HVA reassessments will continue to repreform Risk and Vulnerability Assessments (RVAs) and Security Architecture Reviews (SARs) every three years. DHS' CISA continues to onboard additional assessment staff, streamline processes, and pursue other continuous improvement efforts to ensure that the agency can perform RVAs and SARs at the necessary rate to perform all 212 Tier 1 assessments every 36 months.

CSD is currently conducting a pilot Cyber Qualification Initiative (CQI), which provides a system for non-CISA teams to perform assessment services to the same level of quality as CISA. Once the CQI is out of the pilot phase and is offered to agency teams and third- party assessors (projected Q4 2020), it will become a major element of the guidance provided to agencies regarding Tier 2 and Tier 3 HVAs. ECD: September 30, 2020.

## GAO's Mission

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

## Obtaining Copies of GAO Reports and Testimony

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

### Order by Phone

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

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

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

## Connect with GAO

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

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/fraudnet/fraudnet.htm

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

## Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

## Public Affairs

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

## Strategic Planning and External Liaison

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

Please Print on Recycled Paper.