United States Senate
Committee on Homeland Security and Governmental Affairs

Rob Portman, Ranking Member
Gary Peters, Chairman

FEDERAL CYBERSECURITY: AMERICA'S DATA *STILL* AT RISK

STAFF REPORT

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

UNITED STATES SENATE

August 2021

FEDERAL CYBERSECURITY: AMERICA'S DATA *STILL* AT RISK

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In June 2019, the Permanent Subcommittee on Investigations (Subcommittee) issued a bipartisan report titled: *Federal Cybersecurity: America's Data at Risk* (the 2019 Report). That report highlighted systemic failures of eight key Federal agencies to comply with Federal cybersecurity standards identified by agencies' inspectors general. The 2019 Report documented how none of these eight agencies met basic cybersecurity standards and protocols, including properly protecting Americans' personally identifiable information (PII); maintaining a list of the equipment and programs on agency networks; and promptly installing security patches to remediate vulnerabilities that hackers could exploit. The 2019 Report also highlighted that all eight agencies were operating legacy computer systems, which are costly to maintain and difficult to secure. Based on those findings, the Subcommittee determined that these eight Federal agencies were failing to protect the sensitive data they stored and maintained.

This report revisits those same eight agencies two years later. What this report finds is stark. Inspectors general identified many of the same issues that have plagued Federal agencies for more than a decade. Seven agencies made minimal improvements, and only DHS managed to employ an effective cybersecurity regime for 2020. As such, this report finds that these seven Federal agencies still have not met the basic cybersecurity standards necessary to protect America's sensitive data.

* * * * * * * * * * *

The current state of cyber espionage. In the past two years, state-sponsored hackers have perpetrated some of the largest and most damaging cyber-attacks in our history. In December 2020, we learned that the Russian Foreign Intelligence Service used a sophisticated supply chain vulnerability to corrupt a security patch for SolarWinds network management software. This allowed hackers to infiltrate nine Federal agencies, including DHS, State, Energy, and Treasury. Russia's cyber-spies remained undetected in those Federal agencies' systems for at least nine months. The Federal Government only became aware of the attack after it was discovered by a private cybersecurity firm, FireEye, which was also breached. The Federal Government is still working to understand exactly what information and data Russia accessed during those nine months.

In April 2021, we learned Chinese hackers breached multiple Federal agencies through a vulnerability in a widely used remote access product called Pulse Connect Secure. A Chinese state-sponsored hacking group exploited vulnerabilities in Pulse Connect Secure products allowing hackers to bypass passwords and multifactor authentication to access agencies' data.

These were just two of the most damaging attacks. Indeed, for 2020, the White House reported 30,819 information security incidents across the Federal Government—an 8 percent increase from the prior year.

The 2019 Subcommittee Report. It was no surprise that Federal agencies fell victim to these cyber-attacks. In June 2019, the Subcommittee reported the failures of eight Federal agencies to comply with basic cybersecurity standards. The 2019 Report analyzed a decade (2008–2018) of inspector general audit reports evaluating compliance with Federal statutory cybersecurity

standards for eight agencies: the Departments of (1) Homeland Security (DHS); (2) State (State); (3) Transportation (DOT); (4) Housing and Urban Development (HUD); (5) Agriculture (USDA); (6) Health and Human Services (HHS); (7) Education (ED); and (8) the Social Security Administration (SSA).

The 2019 Report found similar vulnerabilities identified by inspectors general across the eight agencies. In short, inspectors general found:

(1) Seven agencies failed to provide for the adequate protection of PII.

(2) Five agencies failed to maintain accurate and comprehensive IT asset inventories.

(3) Six agencies failed to timely install security patches and other vulnerability remediation actions designed to secure the application.

(4) All eight agencies used legacy systems or applications that are no longer supported by the vendor with security updates resulting in cyber vulnerabilities for the system or application.

Two years later, seven agencies still fail at effectively securing data. In 2021, the Committee sought to determine if the eight agencies made any advancements in their cybersecurity posture over the past two years. Just as before, the Committee reviewed the annual audit findings by the eight agencies' inspectors general for fiscal year 2020. While several of the agencies made minimal improvements in one or more areas, inspectors general found essentially the same failures as the prior 10 years. Only DHS had an effective cybersecurity program for 2020; every other agency failed to implement an effective cybersecurity program.

This has not always been the case for DHS. In FY 2019—the most recent FISMA report available for the Committee to review—the DHS Inspector General assigned the lowest possible rating to DHS for three of the five areas reviewed. To be clear, in FY 2019 the agency responsible for implementing cybersecurity standards across the Federal Government received a failing grade for its own cybersecurity posture. As an example, the DHS Inspector General identified 26 "high vulnerabilities" at three DHS components because it had not applied security patches. High vulnerabilities are considered entry points for hackers to breach an agency's network and ***significantly*** impact operations. The DHS IG has identified the failure to properly apply security patches at DHS for the last 12 years.

Other concerning findings from the FY 2020 inspector general audits include:

- The State Department could not provide documentation for 60 percent of the sample employees tested who had access to the agency's classified network and left thousands of accounts active after an employee left the agency for extended periods of time on both its classified and unclassified networks.

- The Department of Transportation (DOT) Inspector General found 14,935 IT assets belonging to the Department, including 7,231 mobile devices, 4,824 servers, and 2,880 workstations of which the Department had no record.

- The Department of Housing and Urban Development (HUD) Inspector General found unauthorized "shadow IT" on the agency's network that the agency "may not learn of the existence of . . . until it fails or is breached."

- The Department of Agriculture (USDA) Inspector General found a significant number of high vulnerabilities on the agency's public facing websites that were unknown to the agency.

- Two components at the Department of Health and Human Services (HHS) had not fully implemented DHS's flagship cybersecurity programs—a cyber-intrusion detection system known as "EINSTEIN" that identifies known threats to the network and has been required by law for five years, and a program called Continuous Diagnostics and Mitigation, which the Department asserted it could not force its subordinate components to implement.

- In a test of the Department of Education's security, the Inspector General was able to exfiltrate hundreds of sensitive PII files, including 200 credit card numbers without the agency detecting or blocking it.

- Auditors found SSA did not sufficiently protect PII or apply appropriate access management controls—this includes the failure to implement several requirements in the *Federal Cybersecurity Enhancement Act of 2015*.

At least seven of the eight agencies still operated unsupported legacy systems. Only one agency's inspector general did not cite it for continuing to operate legacy information technology in FY 2020, HHS, and the Government Accountability Office has historically noted at least three legacy systems at HHS, including its Medicare Beneficiary Enrollment system.

The inspectors general each assigned a rating to their respective agencies' cybersecurity practices. A rating of 1 is the lowest, which this report defines as an "F." A rating of 5 is the highest, defined in the report as an "A." HUD, USDA, and HHS received Cs. State, DOT, Education, and SSA all received Ds. The highest grade received was a B, awarded to DHS.

It is clear that the data entrusted to these eight key agencies remains at risk. As hackers, both state-sponsored and otherwise, become increasingly sophisticated and persistent, Congress and the executive branch cannot continue to allow PII and national security secrets to remain vulnerable.

FINDINGS AND RECOMMENDATIONS

A. Findings of Fact

(1) According to agency inspectors general, the average grade of the large Federal agencies' overall information security maturity was a C-.

(2) All eight agencies reviewed in depth had significant cybersecurity weaknesses, including:

- Six agencies operated systems without current authorizations to operate.
- Seven agencies used legacy systems or applications no longer supported by the vendor with security updates.
- Six agencies failed to install security patches and other vulnerability remediation controls quickly.
- Seven agencies failed to maintain accurate and comprehensive information technology asset inventories.
- Seven agencies failed to protect PII adequately.

(3) Since the 2019 Portman-Carper report evaluating the same eight agencies, only DHS established an effective information security program. Three agencies—DOT, Education, and SSA—showed very little improvement since the Subcommittee's report in 2019.

(4) There is no single point of accountability for federal cybersecurity. Instead, cybersecurity responsibilities are highly federated making Government-wide information security improvements difficult. Additionally, the Federal Government lacks a unified cybersecurity strategy to combat the current threat landscape.

(5) The DHS Inspector General failed to submit its annual evaluation to Congress prior to this report's release. Of the eight agencies examined by the Committee, the DHS OIG was the only agency which failed to do so.

(6) The Federal Government's continued overreliance on costly and difficult-to-secure legacy technology diverts critical funding away from other security efforts.

(7) DHS's flagship cybersecurity program for Federal agencies—the National Cybersecurity Protection System (NCPS), operationally known as EINSTEIN—suffers from significant limitations in detecting and preventing intrusions.

(8) Agencies consistently failed to implement certain key cybersecurity requirements including encryption of sensitive data, limiting each user's access to the information and systems needed to perform their job, and multi-factor authentication, or to certify to Congress that the system is nonetheless secure.

B. Recommendations

(1) OMB should develop and require agencies to adopt a risk-based budgeting model for information technology investments. Agencies currently use limited technology funds on capabilities for perceived security weaknesses instead of those most likely to be exploited by hostile actors. This risk-based model would address blind information technology spending and provide agencies with a better sense of their return on investment for each capability acquired.

(2) There should be a centrally coordinated approach for Government-wide cybersecurity to ensure accountability. A primary office should coordinate with appropriate agencies to develop and implement a cybersecurity strategy for the Federal Government.

(3) CISA's Cybersecurity Quality Services Management Office should expand shared services offerings to Federal agencies, including improved, Government-wide endpoint detection using primarily commercial off the shelf products and services to improve the operational effectiveness of EINSTEIN. Shared services are often the most time and cost efficient way for agencies to fortify their cyber defenses and strengthen the security posture of Federal networks.

(4) The Department of Homeland Security should provide Congress with a plan to update EINSTEIN and to justify its cost.

(5) The annual *Inspector General FISMA Reporting Metrics* developed by OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency should prioritize risk-based metrics that best demonstrate the maturity of an agency's information security program. Those metrics, among other things, should assess an agency's ability to identify: (1) common threat patterns; (2) security controls that address those common threat patterns; and (3) any other security risks unique to that agency's networks.

(6) Congress should update the *Federal Information Security Modernization Act of 2014*:

- To reflect current cybersecurity best practices, including focusing on mitigating identified and analyzed cybersecurity risks, in addition to meeting compliance risks;
- To formalize CISA's role as the operational lead for Federal cybersecurity;
- To require Federal agencies and contractors notify CISA of certain cyber incidents; and
- To define "major incident" in a way that ensures Federal agencies notify Congress in a timely manner of significant cyber incidents instead of continuing to rely on the current definition which has promoted inconsistent notification to Congress.

I. BACKGROUND

Securing Federal networks has never been more important. Federal agencies maintain the personal information of millions of Americans who have no say in how that information is maintained and protected. Despite legal requirements for Federal agencies to secure their networks, they repeatedly fail to do so—this includes not implementing basic cybersecurity hygiene practices and protecting the sensitive information entrusted to them.[1]

A. The *Federal Information Security Management Act of 2002*

In 1996, GAO identified the risks associated with the Federal Government's increased reliance upon information systems noting agencies "face an increasing challenge to protect the integrity, confidentiality, and availability of the data they maintain."[2] GAO predicted "sensitive and critical information could be inappropriately modified, disclosed, or destroyed, possibly resulting in significant interruptions in service, monetary losses, and a loss of confidence in the [G]overnment's ability to protect confidential data on individuals."[3] GAO also added that although the information held by Federal agencies is often unclassified, it is "extremely sensitive, and many automated operations would be attractive targets for individuals or organizations with malicious intentions . . . ."[4] Consistent with these findings, GAO has designated information security as a high risk area for the Federal Government every year since 1997.[5]

Congress first enacted permanent legal requirements for Federal agency cybersecurity in the *Federal Information Security Management Act of 2002*.[6] This law authorized the expiring information security measures originally contained in the *Government Information Security Reform Act* (GISRA).[7]

As enacted in 2001, GISRA mandated that program managers and Chief Information Officers (CIO) develop a "comprehensive framework for establishing and ensuring the effectiveness of controls over information resources that support Federal operations and assets."[8] In particular, this risk-based security management program had to include:

(1) Periodic risk assessments evaluating internal and external threats;

(2) Training on information security for employees; and

---

[1] *See generally* STAFF OF S. PERMANENT SUBCOMM. ON INVESTIGATIONS, 116TH CONG., REP. ON FEDERAL CYBERSECURITY: AMERICA'S DATA AT RISK (2019).
[2] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO/AIMD 96-110, INFORMATION SECURITY: OPPORTUNITIES FOR IMPROVED OMB OVERSIGHT OF AGENCY PRACTICES 2 (1996).
[3] *Id.*
[4] *Id.*
[5] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 21-119, HIGH RISK SERIES: DEDICATED LEADERSHIP NEEDED TO ADDRESS LIMITED PROGRESS IN MOST HIGH-RISK AREAS 168 (2021).
[6] Federal Information Security Management Act of 2002, Pub. L. No. 107-347, Title III, 116 Stat. 2946, *codified as amended at* 44 U.S.C. § 3541 (2002).
[7] National Defense Authorization Act for Fiscal Year 2001, Pub. L. No. 106-398, Title X, Subtitle G−Government Information Security Reform Act, 114 Stat. 1654A−266, *codified as amended at* 44 U.S.C. §3531 (2000).
[8] *Id.* at 44 U.S.C. § 3531.

(3) The development of procedures for identifying, reporting, and responding to cyber incidents.[9]

That legislation also required each agency to conduct an annual independent evaluation of its information security program.[10] This requirement provided both Congress and OMB with the opportunity to oversee the effectiveness of agency efforts pertaining to information security.[11]

Beyond making GISRA permanent, the *Federal Information Security Management Act of 2002* required the Director of OMB to establish and oversee a central Federal information security incident center and promulgate standards and guidelines pertaining to Federal information systems.[12] The law contained provisions establishing, for the first time, Government-wide minimum mandatory management controls instead of providing each agency with the discretion to set its own minimum controls.[13]

Even after Congress passed the *Federal Information Security Management Act of 2002*, Federal agency information security problems persisted. For example, GAO determined that in FY 2012, 23 out of the 24 major Federal agencies had deficiencies in controls intended to curtail or identify unauthorized access to computer resources.[14] That same GAO report also found that all 24 agencies had security vulnerabilities in the controls intended to prevent "unauthorized changes to information system resources."[15]

These findings, among other concerns, prompted Congress to reevaluate the 2002 law.[16] GAO found information security roles were unclear throughout the Federal Government.[17] For example, although the *Federal Information Security Management Act of 2002* granted OMB the lead statutory authority over Federal cybersecurity, OMB delegated much of that authority to DHS.[18] This created confusion as to which agency was in charge.[19]

In 2014, Congress sought to update the 2002 law due to the increased targeting of vulnerable Government IT systems.[20] Congress also recognized the need for a new approach to Federal cybersecurity because dated and paperwork intensive cybersecurity requirements prevented agencies from implementing modern security practices that would allow them to address

---

[9] *Id.*
[10] *Id.* at 44 U.S.C. § 3535.
[11] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 02-677T, INFORMATION SECURITY: COMMENTS ON THE PROPOSED FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002 8 (2002).
[12] Federal Information Security Management Act of 2002, Pub. L. No. 107-347, Title III, 116 Stat. 2946, *codified as amended at* 44 U.S.C. § 3543 (2002).
[13] *Id.* at 44 U.S.C. § 3544.
[14] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 13-776, FEDERAL INFORMATION SECURITY: MIXED PROGRESS IN IMPLEMENTING PROGRAM COMPONENTS; IMPROVED METRICS NEEDED TO MEASURE EFFECTIVENESS 13 (2013).
[15] *Id.* at 14.
[16] STAFF OF S. PERMANENT SUBCOMM. ON INVESTIGATIONS, 116TH CONG., REP. ON FEDERAL CYBERSECURITY: AMERICA'S DATA AT RISK 18 (2019).
[17] *Id.*
[18] S. Rep. No. 113-256, at 3−5 (2014).
[19] *Id.* at 5.
[20] *Id.* at 2−3.

emerging threats better.[21] To address these weaknesses, Congress enacted the *Federal Information Security Modernization Act of 2014* on December 18, 2014.[22]

B. The *Federal Information Security Modernization Act of 2014*

The *Federal Information Security Modernization Act of 2014* reaffirmed OMB's responsibility to develop and to oversee "the implementation of policies, principles, standards, and guidelines on information security."[23] It also tasked OMB with "overseeing agency compliance with the requirements" in the legislation.[24] Unlike its predecessor, the Act required DHS to "administer the implementation of agency information security policies and practices for information systems."[25]

Under the *Federal Information Security Modernization Act of 2014*, Congress required DHS to develop and to oversee "the implementation of binding operational directives to agencies to implement the policies, principles, standards, and guidelines" set by OMB.[26] A binding operational directive is "a compulsory direction to an agency that is for the purposes of safeguarding Federal information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk."[27] OMB retained the power to revise or repeal these directives if it determined that they are "not in accordance with the policies, principles, standards, and guidelines" developed by OMB.[28]

To promote information security audit uniformity across the Federal Government, the 2014 law required DHS to consult with National Institute of Standards and Technology (NIST) to "ensure that binding operational directives" do not conflict with the information security standards set forth by NIST.[29] This coordination sought to preserve the NIST standards, thereby allowing FISMA compliance to be compared across the Government rather than attempting to reconcile metrics established individually by each agency.[30]

Current law regulating Federal agency cybersecurity, which includes both the *Federal Information Security Management Act of 2002* and the *Federal Information Security Modernization Act of 2014* as amended, is codified at subchapter II of chapter 35, title 44, United States Code (section 3551, *et seq*.), and is commonly referred to as FISMA.[31]

---

[21] *Id.* at 6−7.
[22] Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (2014), *codified as amended at* 44 U.S.C. § 3551.
[23] *Id. at* § 3553(a)(1).
[24] *Id.* at § 3553(a)(5).
[25] *Id.* at § 3553(b).
[26] *Id.* at § 3553(b)(2).
[27] *Id.* at § 3552(b)(1)(A).
[28] *Id.* at § 3553(b)(2).
[29] *Id.* at § 3553(f)(2)(A)−(B).
[30] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 17-549, FEDERAL INFORMATION SECURITY: WEAKNESSES CONTINUE TO INDICATE NEED FOR EFFECTIVE IMPLEMENTATION OF POLICIES AND PRACTICES 46 (2017).
[31] Confusingly, FISMA has been variously used to refer to the originally enacted *Federal Information Security Management Act of 2002*, Pub. L. No. 107-347, 116 Stat. 2946 (2002); the *Federal Information Security Modernization Act of 2014*, Pub. L. 113-283, 128 Stat. 3073 (2014), which amended *Federal Information Security Management Act of 2002*; and subchapter II, chapter 35, title 44, United States Code (44 U.S.C. § 3551, *et seq*), the

To facilitate and streamline the implementation of OMB cybersecurity policies, FISMA required DHS to "[convene] meetings with senior agency officials."[32] These meetings sought to help DHS determine whether it should provide "operational and technical assistance" to an agency to improve information security.[33] The law also required OMB to submit an annual report to Congress detailing "the effectiveness of information security policies and practices during the preceding year."[34] These reports must summarize major cyber incidents from that year and the latest information security program evaluations.[35] In addition, OMB must assess agency compliance with data breach notification procedures established by the OMB Director.[36]

At the agency level, department heads are responsible for prioritizing information security in the budgetary process, ensuring that senior agency officials carry out all FISMA-related responsibilities, and holding agency personnel accountable for information security program violations.[37] Each agency is required to "document, and implement an agency-wide information security program" and conduct periodic assessments to ensure continued efficiency and cost effectiveness.[38] Moreover, like its predecessor, FISMA required that each agency undergo an independent evaluation of its information security program.[39] This evaluation requires each agency to test and assess the "effectiveness of [its] information security policies, procedures, and practices."[40]

The *Federal Information Security Modernization Act of 2014* also shifted responsibility for the operation of the Federal Information Security Incident Center (FISIC) from OMB to DHS and required Federal agencies to report every "major incident" observed on their networks to Congress.[41] OMB defined a major incident as "any incident that is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States."[42] In the event that a major incident occurs, agencies must report that incident no "later than [seven] days after the date on which there is a reasonable basis to conclude that [a] major incident has occurred."[43]

Last, the *Federal Information Security Modernization Act* mandated that OMB update data breach notification guidelines periodically and requires affected agencies to notify Congress "not later than 30 days after the date on which the agency discovered the unauthorized acquisition or

---

positive title of the United States Code in which both statutes were enacted. This report uses "FISMA" to refer to the current law—subchapter II, chapter 35, title 44, United States Code and the full names of the two acts to refer to the freestanding bills.

[32] *Id.* at § 3553(b)(4).
[33] *Id.* at § 3553(b)(6).
[34] *Id.* at § 3553(c).
[35] *Id.* at § 3553(c)(1)−(3).
[36] *Id.* at § 3553(c)(5).
[37] *Id.* at § 3554(a)(1)(A)−(C), (a)(6), (a)(7).
[38] *Id.* at § 3554(b)−(b)(1).
[39] *Id.* at § 3555(a).
[40] *Id.* at § 3555(a)(2)(B).
[41] *Id.* at §§ 3553(b)(6)(A), 3554(b)(7)(C)(iii)(III).
[42] OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, M-21-02, FISCAL YEAR 2020-2021 GUIDANCE ON FEDERAL INFORMATION SECURITY AND PRIVACY MANAGEMENT REQUIREMENTS 5 (2020).
[43] Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (2014), *codified as amended at* 44 U.S.C. § 3554(b)(7)(C)(iii)(III)(aa).

access."[44] This notification must detail the information compromised and estimate the number of individuals affected.[45] Agencies who experience a breach must also notify affected individuals "as expeditiously as practicable and without unreasonable delay after the agency discovers the unauthorized acquisition or access."[46]

1. NIST's Cybersecurity Framework

On December 18, 2014, Congress passed the *Cybersecurity Enhancement Act of 2014*, which updated NIST's role to "facilitate and support the development of a voluntary, consensus-based, industry-led set of standards, guidelines, best practices, methodologies, procedures, and processes to cost-effectively reduce cyber risks to critical infrastructure."[47] The *Cybersecurity Enhancement Act* adopted the definition of "critical infrastructure" in the *USA PATRIOT Act*—"systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[48] These updates addressed the Federal Government's increased reliance upon technology and the corresponding expansion of potential cyber vulnerabilities.[49]

Pursuant to its legislative mandate under the *Cybersecurity Enhancement Act*, NIST released version 1.1 of its *Framework for Improving Critical Infrastructure Cybersecurity* on April 16, 2018.[50] Composed of three parts, the Framework "is a risk-based approach to managing cybersecurity risk."[51] The Framework Core, the most relevant provision for FISMA guidance, "is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors."[52] The Framework Core is composed of five functions—Identify, Protect, Detect, Respond, and Recover.[53] Collectively, these functions "provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk."[54]

With the Framework, NIST sought to improve organizational risk management—"the ongoing process of identifying, assessing, and responding to risk."[55] Specifically, the Framework uses risk management processes "to enable organizations to inform and prioritize decisions regarding

---

[44] *Id.* at Pub. L. No. 113-283 § 2(d), 128 Stat. 3085 (2014), *codified as amended at* 44 U.S.C. § 3553 note.
[45] *Id.*
[46] *Id.*
[47] Cybersecurity Enhancement Act of 2014, Pub. L. No. 113-274, 128 Stat. 2971 (2014).
[48] USA PATRIOT Act, Pub. L. No. 107-56, 42 U.S.C. § 5195c(e).
[49] *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*, NAT. INST. OF STANDARDS & TECHNOLOGY, 1 (Apr. 16, 2018).
[50] Cybersecurity Enhancement Act of 2014, Pub. L. No. 113-274, 128 Stat. 2971 (2014); Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 44 U.S.C. § 3553(a)(4); *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*, NAT. INST. OF STANDARDS & TECHNOLOGY, 1 (Apr. 16, 2018).
[51] *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*, NAT. INST. OF STANDARDS & TECHNOLOGY, 3 (Apr. 16, 2018).
[52] *Id.*
[53] *Id.*
[54] *Id.*
[55] *Id.* at 4.

cybersecurity."[56] Moreover, it encourages frequent risk assessments "to help organizations select target states for cybersecurity activities that reflect desired outcomes."[57]

2. OMB and DHS Guidance to Agencies for FISMA Compliance

FISMA required OMB and DHS to develop and to administer guidelines applicable to all federal agencies for FISMA compliance. To accomplish this, OMB established definitions for key terms like "major incident," and DHS developed performance metrics that align with the five functions of NIST's Cybersecurity Framework.

On November 9, 2020, OMB issued Memorandum M-21-02, *Fiscal Year 2020–2021 Guidance on Federal Information Security and Privacy Management Requirements*.[58] This memorandum provided reporting guidance and deadlines for Federal agencies' annual FISMA obligations.[59] These reporting deadlines require that all civilian agencies submit annual FISMA reports to OMB and DHS by October 29.[60] Agency reports are then due to Congress and GAO by March 1.[61]

In addition to the annual report, Memorandum M-21-02 required each agency head to submit a letter to the OMB Director and the Secretary of Homeland Security with: (1) a detailed evaluation of the effectiveness of the agency's information security program, (2) details on the total number of incidents reported to the United States Computer Emergency Readiness Team (US-CERT) by the agency, and (3) a description of each major incident encountered by the agency for the preceding year.[62]

FISMA also directed OMB to define the term "major incident" for agency reporting to Congress.[63] OMB subsequently defined a major incident to include "any incident that is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States."[64] Memorandum M-21-02 further provides that a breach involving personally identifiable information (PII) constitutes a major incident when it involves PII "that, if exfiltrated, modified, deleted, or otherwise compromised" would be damaging to the interests of the United States.[65] Agencies are to assess breaches on a case-by-case basis, but a major incident determination is required "for any unauthorized modification of, unauthorized deletion of, unauthorized exfiltration of, or unauthorized access to the PII of 100,000 or more people."[66]

---

[56] *Id.*
[57] *Id.*
[58] OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, M-21-02, FISCAL YEAR 2020-2021 GUIDANCE ON FEDERAL INFORMATION SECURITY AND PRIVACY MANAGEMENT REQUIREMENTS 1 (2020).
[59] *Id.* at 3.
[60] *Id.*
[61] *Id.* at 4.
[62] *Id.* at 3−4.
[63] Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 44 U.S.C. § 3558(b).
[64] OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, M-21-02, FISCAL YEAR 2020-2021 GUIDANCE ON FEDERAL INFORMATION SECURITY AND PRIVACY MANAGEMENT REQUIREMENTS 5 (2020).
[65] *Id.* at 5−6.
[66] *Id.* at 6.

OMB guidance also reiterates FISMA's requirement that in the event of a major incident an agency must notify Congress within seven days.[67]

To supplement OMB's FISMA guidance, DHS establishes general FISMA metrics each fiscal year. This document assists each agency inspector general in the annual information security evaluation required by FISMA. In particular, these metrics "provide reporting requirements across key areas to be addressed in the independent evaluations."[68] The list below provides an overview of each DHS metric's alignment with NIST's Cybersecurity Framework and its five security functions:

(1) Identify (Asset Management; System Authorization);

(2) Protect (Remote Access Protection; Credentialing and Authorization; Configuration and Vulnerability Management; HVA Protection);

(3) Detect (Intrusion Detection and Prevention; Exfiltration and Enhanced Defenses);

(4) Respond; and

(5) Recover.[69]

Using these metrics, inspectors general must rate their agencies on each of the five functions contained in NIST's Cybersecurity Framework.[70] These ratings aim to "capture the extent that agencies institutionalize" the requirements set forth in FISMA.[71]

For the purposes of this maturity model, if an agency achieves a Level 4, "Managed and Measurable" rating, it is considered effective.[72] When assessing the agency's overall information security program effectiveness, DHS guidance encourages inspectors general to apply a simple majority rule.[73] Under this rule, if at least three of the five security functions receive a Level 4 rating, that agency's information security program is considered effective.[74]

The table below summarizes the five possible maturity ratings and their corresponding descriptions.

[67] *Id.* at 7.
[68] U.S. DEP'T OF HOMELAND SEC., FY 2020 INSPECTOR GENERAL FISMA REPORTING METRICS 4.0, at 4 (2020).
[69] OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014: ANNUAL REPORT TO CONGRESS 40 (2020).
[70] U.S. DEP'T OF HOMELAND SEC., FY 2020 INSPECTOR GENERAL FISMA REPORTING METRICS 4.0, at 4 (2020).
[71] *Id.* at 5.
[72] U.S. DEP'T OF HOMELAND SEC., FY 2020 INSPECTOR GENERAL FISMA REPORTING METRICS 4.0, at 6 (2020).
[73] *Id.*
[74] *Id.*

Maturity Level	Maturity Level Description
Level 1: Ad-hoc	Policies, procedures, and strategies are not formalized; activities are performed in an ad-hoc, reactive manner
Level 2: Defined	Policies, procedures, and strategies are formalized and documented but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4: Managed and Measureable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies are collected across the organizations and used to assess them and make necessary changes.
Level 5: Optimized	Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, consistently implemented and regularly updated based on a changing threat and technology landscape and business/mission needs.

NIST Cybersecurity Framework Maturity Ratings
Source: OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014: ANNUAL REPORT TO CONGRESS FY 2020 at 41 (2020).

3. Oversight of Agency Compliance with FISMA

To ensure agency accountability, Congress imposed deadlines and oversight requirements in FISMA, including the previously discussed requirement that agency inspectors general evaluate their agency's information security program.[75] This requirement was a holdover from the 2002 law.[76] This evaluation must include both testing and an assessment of "the effectiveness of the information security policies, procedures, and practices" of the agency and its information systems.[77] Congress also instructed GAO to provide periodic reports evaluating agency information security programs and the implementation of FISMA requirements.[78] Since the passage of the *Federal Information Security Management Act of 2002* and continuing with the

[75] Federal Information Security Modernization Act of 2014, *codified as amended at* 44 U.S.C. § 3555.
[76] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 02-677T, INFORMATION SECURITY: COMMENTS ON THE PROPOSED FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002 6 (2002).
[77] Federal Information Security Modernization Act of 2014 § 3555(a)(2)(A)−(B).
[78] *Id.* at § 3555(h)(1)−(2).

Federal Information Security Modernization Act of 2014, each inspector general issues an annual report documenting agency compliance and implementation efforts.

FISMA also authorized GAO to provide technical assistance to agency heads or agency inspectors general.[79] In this role, GAO assists agency officials in carrying out FISMA mandates "by testing information security controls and procedures."[80]

C. The *Federal Cybersecurity Enhancement Act of 2015*, National Cybersecurity Protection System, and Continuous Diagnostics and Mitigation Program

On December 18, 2015, Congress passed the *Federal Cybersecurity Enhancement Act of 2015* as part of the *Consolidated Appropriations Act, 2016*.[81] This law authorized DHS to establish and deploy an intrusion detection and intrusion prevention system to identify risks "in network traffic transiting or traveling to or from an agency information system."[82] Moreover, the law mandated DHS make those capabilities available to all Federal agencies and required agencies to implement them.[83] That system, the National Cybersecurity Protection System (NCPS), is operationally known as EINSTEIN. EINSTEIN, together with DHS's Continuous Diagnostics and Mitigation (CDM) program constitute the Department's two flagship programs to improve the Federal Government's cybersecurity posture.[84]

Finally, the *Federal Cybersecurity Enhancement Act of 2015* gave Federal agencies one year to comply with a series of additional cybersecurity requirements.[85] These requirements included the: (1) identification of sensitive and mission critical data held by the agency, (2) assessment of access controls to ensure least privilege and adequate network segmentation, (3) encryption of data stored or transiting agency systems, (4) implementation of login.gov for logons to Federal Government websites by members of the public; and (5) implementation of multi-factor authentication for remote access and users with elevated privileges on agency systems.[86] These requirements, however, can be waived if an agency head personally certifies that the implementation of a requirement would be excessively burdensome, the requirement is not necessary to secure agency systems, and the agency has taken all necessary steps to secure agency systems.[87] The law requires these certifications be submitted to Congress.[88] To date Committee staff are not aware of any agency ever submitting a certification, meaning any agency

---

[79] *Id.* at § 3555(i).
[80] *Id.*
[81] Federal Cybersecurity Enhancement Act of 2015, Pub. L. No. 114-113, Div. N, Title II, Subtitle B, 129 Stat. 2963 (2015).
[82] *Id.* at § 230(b)(1)(A), *codified as amended at* 6 U.S.C § 151.
[83] *Id.*
[84] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 19-105, INFORMATION SECURITY: AGENCIES NEED TO IMPROVE IMPLEMENTATION OF FEDERAL APPROACH TO SECURING SYSTEMS AND PROTECTING AGAINST INTRUSIONS 13 (2018).
[85] Consolidated Appropriations Act, Pub. L. No. 114-113 § 225, Title II, Subtitle B−Federal Cybersecurity Enhancement Act, 129 Stat. 2967 (2015), 6 U.S.C. § 1501.
[86] Consolidated Appropriations Act, Pub. L. No. 114-113 § 225(b)(1), Title II, Subtitle B−Federal Cybersecurity Enhancement Act, 129 Stat. 2967 (2015), 6 U.S.C. § 1501.
[87] Consolidated Appropriations Act, Pub. L. No. 114-113 § 225(b)(2), Title II, Subtitle B−Federal Cybersecurity Enhancement Act, 129 Stat. 2963, 2968 (2015), 6 U.S.C. § 1501.
[88] *Id.*

that does not encrypt its sensitive data or implement multi-factor authentication is not in compliance with the law.

1. National Cybersecurity Protection System

DHS describes NCPS as "an integrated system-of-systems that delivers a range of capabilities, such as intrusion detection, analytics, information sharing, and intrusion prevention."[89] Composed of three separate, yet complementary capabilities, NCPS, is designed to "provide a technological foundation that enables [DHS] to secure and defend the Federal Civilian Executive Branch agencies' information technology infrastructure against advanced cyber threats."[90]

The following table summarizes each NCPS capability:

Table 1: Overview of the National Cybersecurity Protection System (NCPS) Deployment, 2003-2013

Operational name	Deployment year	NCPS objective	Description
EINSTEIN 1	2003	Intrusion detection	Provides an automated process for collecting, correlating, and analyzing agencies' computer network traffic information from sensors installed at their Internet connections.[a]
EINSTEIN 2	2009	Intrusion detection	Monitors federal agency Internet connections for specific predefined signatures of known malicious activity and alerts DHS's U.S. Computer Emergency Readiness Team (US-CERT) when specific network activity matching the predetermined signatures is detected.[b]
EINSTEIN 3 Accelerated	2013	Intrusion detection Intrusion prevention	Automatically blocks malicious traffic from entering or leaving federal civilian agency networks. This capability is managed by Internet service providers, who administer intrusion prevention and threat-based decision making using DHS-developed indicators of malicious cyber activity to develop signatures.[c]

Source: GAO analysis of Department of Homeland Security (DHS) data. | GAO-19-105

[a]The network traffic information includes source and destination Internet Protocol addresses used in the communication, source and destination ports, the time the communication occurred, and the protocol used to communicate.

[b]Signatures are recognizable, distinguishing patterns associated with cyberattacks, such as a binary string associated with a computer virus or a particular set of keystrokes used to gain unauthorized access to a system.

[c]An indicator is defined by DHS as human-readable cyber data used to identify some form of malicious cyber activity. These data may be related to Internet Protocol addresses, domains, e-mail headers, files, and character strings. Indicators can be either classified or unclassified.

Capabilities of the National Cybersecurity Protection System (NCPS), also known as EINSTEIN. Source: U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 19-105, INFORMATION SECURITY: AGENCIES NEED TO IMPROVE IMPLEMENTATION OF FEDERAL APPROACH TO SECURING SYSTEMS AND PROTECTING AGAINST INTRUSIONS 14 (2018).

NCPS largely relies on something called signature-based detection to detect hackers,[91] the digital equivalent of using hacker fingerprints and their tradecraft previously seen on one computer, to detect them on other computers in the future. In January 2016, GAO issued a report outlining several shortcomings with NCPS. For example, of the five software applications reviewed by

[89] *National Cybersecurity Protection System (NCPS)*, U.S. DEP'T OF HOMELAND SEC., https://www.dhs.gov/national-cybersecurity-protection-system-ncps.
[90] *Id.*
[91] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 16-294, INFORMATION SECURITY: DHS NEEDS TO ENHANCE CAPABILITIES, IMPROVE PLANNING, AND SUPPORT GREATER ADOPTION OF ITS NATIONAL CYBERSECURITY PROTECTION SYSTEM 16 (2016).

GAO, NCPS intrusion detection signatures "provided some degree of coverage" for roughly 29 of 489 vulnerabilities identified—roughly six percent.[92] This is problematic because signature based detection is a simple but effective tool for detecting known vulnerabilities and previously seen malicious actors and their established tactics, techniques, and procedures.[93]

But signature based detection does have its limitations—most notably its inability to detect malicious activity never seen before. Just as the police would not have fingerprints to identify a burglar they had never seen before, NCPS generally cannot detect a hacker no one has seen before. Even known hackers can take easy steps to disguise their fingerprints—changing their tactics, techniques, and procedures as easily as a burglar might don gloves. As an example of the limitations of signature-based intrusion detection systems, NCPS is unable to detect malicious actors who use encryption "because NCPS cannot decrypt that traffic to peer into it and look for bad actors and malware."[94] Yet "more than 90 percent of traffic in [the] Federal Government is encrypted."[95] NCPS also cannot detect "zero days" which are vulnerabilities not yet publicly disclosed or otherwise unknown to DHS.[96] In authorizing NCPS, Congress required DHS to make improvements to NCPS to address some of these shortcomings with signature-based intrusion detection systems, including "non-signature based detection technologies, like heuristic and behavior-based detection technologies."[97] This requirement sought to address NCPS's fundamental weakness and improve the system's detection capabilities to extend to unknown threats. Heuristic and behavior-based detection technologies rely on machine-learning and artificial intelligence to spot suspicious activity even if it does not come from a known actor. It might detect, for example, someone logging into work at 3:00 a.m. or from a foreign country, when that individual normally only logs into his computer at 9:00 a.m. from his office in Columbus, Ohio. The Act also required DHS to "regularly deploy new technologies and modify existing technologies for [NCPS] and to assess and use commercial and non-commercial technologies to improve detection and prevention capabilities."[98]

Despite these requirements, GAO determined that as of 2016, NCPS relied exclusively on signature-based methodologies for intrusion detection and intrusion prevention.[99] This detracts from the program's overall effectiveness because "NCPS is unable to detect intrusions for which it does not have a valid or active signature deployed."[100] In other words, NCPS did not have the

---

[92] *Id.* at 22.
[93] *See, e.g.*, *id.* at 17.
[94] STAFF OF S. COMM. ON HOMELAND SEC. & GOVERNMENTAL AFFAIRS, 113TH CONG., A REVIEW OF THE DEPARTMENT OF HOMELAND SECURITY'S MISSIONS AND PERFORMANCE 85 (2015).
[95] *Understanding and Responding to the SolarWinds Supply Chain Attack: The Federal Perspective Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 117th Cong. (2021) (testimony of Brandon Wales, Acting Director, CISA).
[96] STAFF OF S. COMM. ON HOMELAND SEC. & GOVERNMENTAL AFFAIRS, 113TH CONG., A REVIEW OF THE DEPARTMENT OF HOMELAND SECURITY'S MISSIONS AND PERFORMANCE 85 (2015).
[97] S. REP. NO. 114-378, at 4 (2015).
[98] *Id.*
[99] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 16-294, INFORMATION SECURITY: DHS NEEDS TO ENHANCE CAPABILITIES, IMPROVE PLANNING, AND SUPPORT GREATER ADOPTION OF ITS NATIONAL CYBERSECURITY PROTECTION SYSTEM 17 (2016).
[100] *Id.* at 17−18.

capability to detect new, previously unseen adversaries or novel tactics, techniques, and procedures.

In 2018, GAO followed up on the issues it highlighted in 2016 and determined that DHS had made improvements to NCPS.[101] During this review, DHS told GAO that it was now "operationalizing functionality intended to identify malicious activity in the network traffic otherwise missed by signature-based methods."[102] DHS also improved the tool it uses to track signatures "to include a mechanism to clearly link signatures to publicly available, open-source information."[103]

Despite these improvements, GAO identified NCPS shortcomings, including NCPS's inability "to effectively detect intrusions across multiple types of traffic."[104]

The *Federal Cybersecurity Enhancement Act of 2015* also required DHS to develop metrics for evaluating the effectiveness of NCPS in detecting and preventing intrusions.[105] Beyond developing these metrics, DHS also must report to Congress annually on the implementation status of intrusion detection and prevention capabilities.[106] Among other things, these reports must specify the technologies used to detect and prevent cybersecurity risks in network traffic, the indicators used to detect cybersecurity risks, and the number of instances when detection and prevention technologies detected risks in network traffic.[107]

GAO found DHS had not instituted metrics for NCPS that provide the Department with "information about how well the system is enhancing government information security."[108] These metrics are key to understanding the added value of NCPS relative to, for example, a commercial off the shelf-solution.[109]

NCPS comes with a significant cost. As of 2020, the projected lifecycle cost of NCPS was roughly $6.4 billion.[110] For FY 2021 alone, Congress appropriated $371 million for NCPS.[111]

When authorizing NCPS in 2015, Congress required that the system be deployed and implemented at all civilian agencies within one year.[112] As of November 2020, CISA reported

---

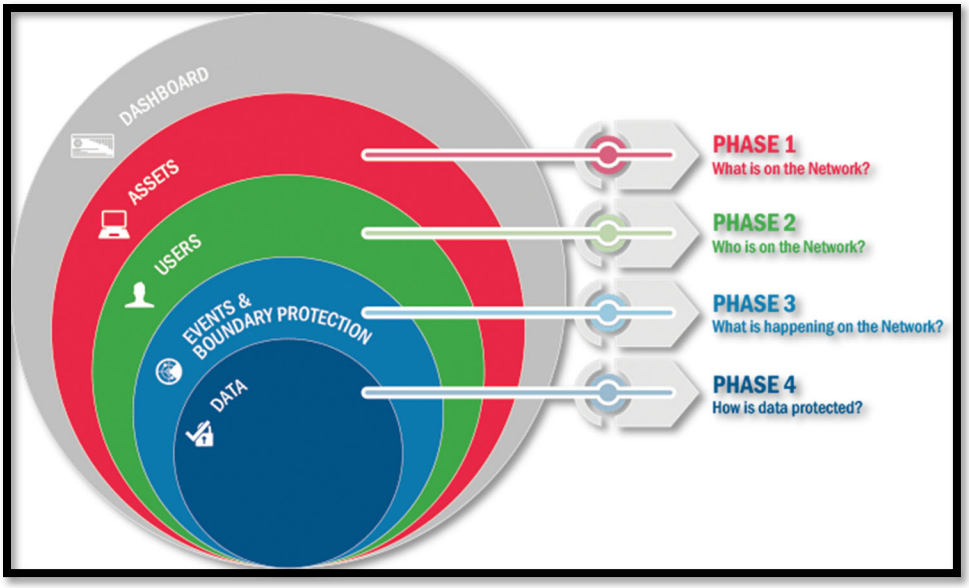
[101] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 19-105, INFORMATION SECURITY: AGENCIES NEED TO IMPROVE IMPLEMENTATION OF FEDERAL APPROACH TO SECURING SYSTEMS AND PROTECTING AGAINST INTRUSIONS 33 (2018).
[102] *Id.*
[103] *Id.* at 34.
[104] *Id.*
[105] Consolidated Appropriations Act, Pub. L. No. 114-113 § 224, Title II, Subtitle B−Federal Cybersecurity Enhancement Act, 129 Stat. 2967 (2015), 6 U.S.C. § 1501.
[106] Consolidated Appropriations Act, Pub. L. No. 114-113 § 226, Title II, Subtitle B−Federal Cybersecurity Enhancement Act, 129 Stat. 2969 (2015), 6 U.S.C. § 1501.
[107] Consolidated Appropriations Act, Pub. L. No. 114-113 § 226, Title II, Subtitle B−Federal Cybersecurity Enhancement Act, 129 Stat. 2969 (2015), 6 U.S.C. § 1501.
[108] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 19-105, INFORMATION SECURITY: AGENCIES NEED TO IMPROVE IMPLEMENTATION OF FEDERAL APPROACH TO SECURING SYSTEMS AND PROTECTING AGAINST INTRUSIONS 35 (2018).
[109] *Id.*
[110] *Id.* at 14.
[111] U.S. DEP'T OF HOMELAND SEC., CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY BUDGET OVERVIEW: FISCAL YEAR 2021 CONGRESSIONAL JUSTIFICATION 14 (2020).
[112] S. REP. NO. 114-378, at 4 (2015).

99 percent of Federal civilian agencies and departments had fully implemented EINSTEIN 3 Accelerated.[113] In recent testimony before the House Appropriations Subcommittee on Homeland Security, CISA Executive Director Eric Goldstein commented on NCPS saying, "the EINSTEIN technology that was reasonably designed to address risks and technology a decade ago has grown somewhat stale over time and now does not provide the visibility that CISA needs."[114]

2. Continuous Diagnostics and Mitigation

NCPS's companion program, CDM, "was developed in 2012 to support government-wide and agency-specific efforts to provide risk-based, consistent, and cost-effective cybersecurity solutions to protect federal civilian networks."[115] CDM aims to reduce agency threat surface, improve incident response, and increase visibility across federal networks.[116]

CDM's tools include sensors that conduct automated scans for known vulnerabilities, the results of which are included on a dashboard that can be accessed by network managers.[117] This dashboard then helps agencies allocate resources for each identified vulnerability.[118] The chart below illustrates the four phases of the CDM program.



Phases of the Continuous Diagnostics and Mitigation Program (CDM)
Source: Continuous Diagnostics and Mitigation (CDM) Capabilities, U.S. DEP'T OF HOMELAND SEC., cisa.gov/cdm.

---

[113] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 21-175, DHS ANNUAL ASSESSMENT: MOST ACQUISITION PROGRAMS ARE MEETING GOALS BUT DATA PROVIDED TO CONGRESS LACKS CONTEXT NEEDED FOR EFFECTIVE OVERSIGHT 34 (2021).
[114] *Modernizing the Federal Civilian Approach to Cybersecurity: Hearing Before the Subcomm. on the Department of Homeland Security of the H. Comm. on Appropriations*, 117th Cong. (2021) (testimony of Eric Goldstein, Exec. Ass't Dir. For Cybersecurity, CISA).
[115] *Continuous Diagnostics and Mitigation (CDM)*, U.S. DEP'T OF HOMELAND SEC., https://www.cisa.gov/cdm.
[116] *Id.*
[117] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 19-105, INFORMATION SECURITY: AGENCIES NEED TO IMPROVE IMPLEMENTATION OF FEDERAL APPROACH TO SECURING SYSTEMS AND PROTECTING AGAINST INTRUSIONS 15 (2018).
[118] *Id.*

Although DHS worked to implement several of the phases shown above, GAO recently concluded that DHS failed to meet the planned implementation dates for each phase.[119] Nearly four years ago, DHS projected that Phase 3 would be completed at 97 percent of federal agencies.[120] DHS, however, did not meet this expectation and has not yet fully implemented Phase 2.[121] Implementation of Phases 3 and 4 is not expected to begin until fiscal years 2022 and 2023.[122]

II. CYBERSECURITY VULNERABILITIES ACROSS THE FEDERAL GOVERNMENT

In 2019, the Senate Permanent Subcommittee on Investigations (Subcommittee) issued a bipartisan report documenting the Federal Government's failure to adhere to information security requirements under FISMA.[123] Among other things, the Subcommittee determined Federal agencies failed to: (1) adequately protect personally identifiable information; (2) maintain accurate and comprehensive IT asset inventories; (3) timely install security patches; and (4) retire legacy technology no longer supported by the vendor.[124]

The report card below offers a broad view of the current state of cybersecurity at most of the largest Federal agencies—the Cabinet departments and other large agencies named in the *Chief Financial Officers Act* whose FISMA reports are unclassified. Each agency was assigned a letter grade on a scale of "A" to "F." These grades correspond directly to one of the five numerical ratings agencies receive from inspectors general. For instance, if an agency received a Level 5, "Optimized" rating from its inspector general (the highest possible rating) that would correspond to an "A".

> ***Inspectors general reported that the vast majority of Federal agencies had ineffective information security programs, leaving their critical data at risk.***

No agency earned an A for their cybersecurity program. Of the 23 agencies in the table, only five—the Department of Homeland Security, the United States Agency for International Development, National Science Foundation, Nuclear Regulatory Commission, and General Services Administration—implemented effective information security programs in accordance with FISMA. Inspectors general reported that the vast majority of Federal agencies had ineffective information security programs, leaving their critical data at risk.

---

[119] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 19-105, INFORMATION SECURITY: AGENCIES NEED TO IMPROVE IMPLEMENTATION OF FEDERAL APPROACH TO SECURING SYSTEMS AND PROTECTING AGAINST INTRUSIONS 38−39 (2018).
[120] *Id.* at 38.
[121] *Modernizing the Federal Civilian Approach to Cybersecurity: Hearing Before the Subcomm. on the Dep't of Homeland Sec. of the H. Comm. on Appropriations*, 117th Cong. (2021) (statement of Brandon Wales, Acting Director, CISA).
[122] *Id.*
[123] STAFF OF S. PERMANENT SUBCOMM. ON INVESTIGATIONS, 116TH CONG., REP. ON FEDERAL CYBERSECURITY: AMERICA'S DATA AT RISK (2019).
[124] *Id.*

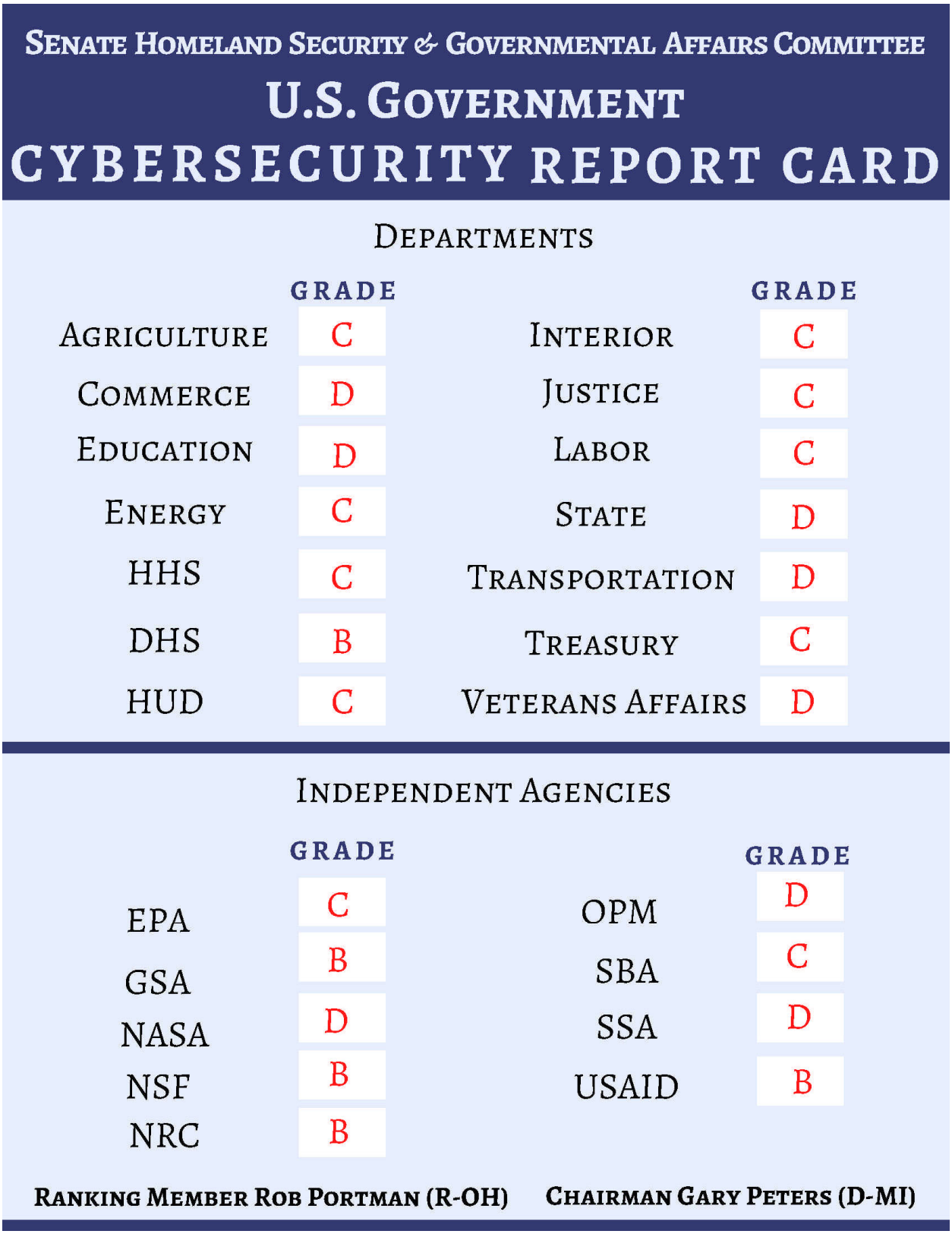


Figure 3: CFO Act Agency Information Maturity Grades
Source: OFF. OF MGMT. & BUDGET, EXEC. OFF. OF THE PRESIDENT, FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 ANNUAL REPORT TO CONGRESS FISCAL YEAR 2020 (2021).

The section below evaluates the current FISMA compliance of several of those agencies above—the eight agencies featured in the Subcommittee's 2019 report. It provides greater detail on the most recent FISMA reports for each agency featured in the Subcommittee's 2019 report and related persistent cybersecurity weaknesses. Those eight agencies are: DHS; State; DOT; HUD; USDA; HHS; ED; and SSA. Based on the Committee's review of FISMA reports by agency inspectors general for FY 2020, only DHS has an effective information security program under FISMA. Three of these agencies—DOT, Education, and SSA—showed very little improvement since the Subcommittee's report in 2019.

A. The Department of Homeland Security

DHS's statutory mission is to prevent, reduce the vulnerability of, and assist in the recovery from terrorist attacks in the United States.[125] DHS describes its mission as the duty to ensure "with honor and integrity, we will safeguard the American people, our homeland, and our values."[126] In particular, DHS identifies six core missions: (1) countering terrorism and homeland security threats; (2) securing U.S. borders; (3) securing cyberspace and critical infrastructure; (4) preserving prosperity and economic security; (5) strengthening preparedness and resilience; and (6) championing the DHS workforce and strengthening the department.[127]

DHS has over a dozen components with sensitive national-security related missions, including the Cybersecurity and Infrastructure Security Agency (CISA), Customs and Border Protection (CBP), the Federal Emergency Management Agency (FEMA), and the Secret Service.[128] Each of these agencies handles sensitive data. For example, CISA is the agency operationally responsible for ensuring cybersecurity across the Federal Government.[129] The Secret Service has sensitive information on the location and protection of the President and other dignitaries.[130] DHS's Countering Weapons of Mass Destruction Office has sensitive information regarding detection and defenses to chemical, biological, radiological, and nuclear threats.[131] The Chemical Facility Anti-Terrorism Standards (CFATS) Program has chemical vulnerability information regarding the quantities and locations of hazardous chemicals around the country—chemicals terrorists might use "to inflict mass casualties in the United States."[132] These agencies also handle PII. For example, CBP's TECS system is the "principal system used by officers at

[125] Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135, 6 U.S.C. § 111 (2002).
[126] *Our Mission*, U.S. DEP'T OF HOMELAND SEC., https://www.dhs.gov/our-mission.
[127] *Strategic Planning*, U.S. DEP'T OF HOMELAND SEC., https://www.dhs.gov/strategic-planning.
[128] *Operational and Support Components*, U.S. DEP'T OF HOMELAND SEC., https://www.dhs.gov/operational-and-support-components.
[129] *Cybersecurity Division Mission and Vision*, CYBERSEC. & INFRASTRUCTURE SEC. AGENCY, U.S. DEP'T OF HOMELAND SEC., https://www.cisa.gov/cybersecurity-division.
[130] *About Us*, U.S. SECRET SERV., https://www.secretservice.gov/about/overview.
[131] *Countering Weapons of Mass Destruction Office*, U.S. DEP'T OF HOMELAND SEC., https://www.dhs.gov/countering-weapons-mass-destruction-office
[132] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 19-402T, CRITICAL INFRASTRUCTURE PROTECTION: PROGRESS AND CHALLENGES IN DHS'S MANAGEMENT OF ITS CHEMICAL FACILITY SECURITY PROGRAM 1 (2019).

the border to assist with screening and determinations regarding admissibility of arriving persons."[133]

While OMB's Government-wide report indicates DHS's information security program was effective in FY 2020, the DHS Inspector General audit was not available for the Committee to examine at the time of this report's release. Therefore, the Committee's review was based on the DHS Inspector General's FY 2019 audit.

DHS's information security program was ineffective for FY 2019—taking a step back from its effective rating in 2018.[134] In fact, DHS received Level 1, "Ad Hoc," ratings in three of five function areas.[135] This is the lowest possible rating under NIST standards, effectively a letter grade of F.[136]

The Inspector General documented DHS's failure to apply security patches in twelve consecutive FISMA audits.

Lack of Valid Authorities to Operate. Auditors identified DHS weaknesses in risk management, and specifically component systems operating with expired authorities to operate.[137] For instance, unclassified systems operating without ATOs more than tripled from FY 2018 to FY 2019.[138] Out of 597 total systems at the Department, 81 were operating without ATOs.[139] The Inspector General has identified this issue every year since 2011.[140]

Use of Unsupported Systems. During its review, the Inspector General noted DHS's use of unsupported information technology.[141] At one DHS component, an unsupported version of

[133] U.S. DEP'T OF HOMELAND SEC., DHS/CBP/PIA-009(A), TECS SYSTEM: CBP PRIMARY AND SECONDARY PROCESSING (TECS) NATIONAL SAR INITIATIVE 2 (2011).
[134] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOMELAND SEC., OIG 20-77, EVALUATION OF DHS' INFORMATION SECURITY PROGRAM FOR FY 2019 6 (2020).
[135] *Id.*
[136] *Id.* at 4.
[137] *Id.* at 13−14.
[138] *Id.* at 18.
[139] *Id.*
[140] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOMELAND SEC., OIG 11-113, EVALUATION OF DHS' INFORMATION SECURITY PROGRAM FOR FY 2011 6 (2011); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOMELAND SEC., OIG 13-04, EVALUATION OF DHS' INFORMATION SECURITY PROGRAM FOR FY 2012 8 (2012); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOMELAND SEC., OIG 14-09, EVALUATION OF DHS' INFORMATION SECURITY PROGRAM FOR FY 2013 5 (2013); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOMELAND SEC., OIG 15-16, EVALUATION OF DHS' INFORMATION SECURITY PROGRAM FOR FY 2014 4 (2014); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOMELAND SEC., OIG 16-08, EVALUATION OF DHS' INFORMATION SECURITY PROGRAM FOR FY 2015 9 (2016); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOMELAND SEC., OIG 17-24, EVALUATION OF DHS' INFORMATION SECURITY PROGRAM FOR FY 2016, DHS OIG HIGHLIGHTS 5 (2017); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOMELAND SEC., OIG 18-56, EVALUATION OF DHS' INFORMATION SECURITY PROGRAM FOR FY 2017 5 (2018); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOMELAND SEC., OIG 19-60, EVALUATION OF DHS' INFORMATION SECURITY PROGRAM FOR FY 2018 10 (2018); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOMELAND SEC., OIG 20-77, EVALUATION OF DHS' INFORMATION SECURITY PROGRAM FOR FY 2019 18 (2020).
[141] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOMELAND SEC., OIG 20-77, EVALUATION OF DHS' INFORMATION SECURITY PROGRAM FOR FY 2019 21 (2020).

Windows was still in use at 184 workstations.[142] Microsoft stopped supporting this version of Windows several years ago.[143] The Inspector General cited DHS's use of unsupported systems in *six* consecutive FISMA audits.[144]

Failure to Remediate Vulnerabilities. In a survey of three DHS components, auditors discovered 26 unique high vulnerabilities.[145] "High vulnerabilities" are weaknesses "in an information system, system security procedures, internal controls, or implementation" that can serve as an entry point for hackers to breach an agency's network and significantly impact operations.[146] Without these patches, "vulnerabilities could result in significant data loss or system disruption."[147] The Inspector General documented DHS's failure to apply security patches in *twelve* consecutive FISMA audits.[148]

Failure to Compile an Accurate and Comprehensive IT Asset Inventory. In 2019, the DHS CIO permitted the Coast Guard to submit its FISMA information to the Department of Defense rather than DHS.[149] As a result, "DHS [was] not able to maintain a comprehensive and accurate

---

[142] *Id.*
[143] *Id.*
[144] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOMELAND SEC., OIG 15-16, EVALUATION OF DHS' INFORMATION SECURITY PROGRAM FOR FY 2014 17 (2014); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOMELAND SEC., OIG 16-08, EVALUATION OF DHS' INFORMATION SECURITY PROGRAM FOR FY 2015 8,10,20 (2016); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOMELAND SEC., OIG 17-24, EVALUATION OF DHS' INFORMATION SECURITY PROGRAM FOR FY 2016, DHS OIG HIGHLIGHTS 11-12 (2017); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOMELAND SEC., OIG 18-56, EVALUATION OF DHS' INFORMATION SECURITY PROGRAM FOR FY 2017 10,12 (2018); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOMELAND SEC., OIG 19-60, EVALUATION OF DHS' INFORMATION SECURITY PROGRAM FOR FY 2018 14 (2018); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOMELAND SEC., OIG 20-77, EVALUATION OF DHS' INFORMATION SECURITY PROGRAM FOR FY 2019 21 (2020).
[145] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOMELAND SEC., OIG 20-77, EVALUATION OF DHS' INFORMATION SECURITY PROGRAM FOR FY 2019 22 (2020).
[146] *Vulnerability*, NIST COMPUTER SEC. RESOURCE CENTER GLOSSARY, https://csrc nist.gov/glossary/term/vulnerability.
[147] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOMELAND SEC., OIG 20-77, EVALUATION OF DHS' INFORMATION SECURITY PROGRAM FOR FY 2019 22 (2020).
[148] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOMELAND SEC., OIG 08-94, EVALUATION OF DHS' INFORMATION SECURITY PROGRAM FOR FY 2008 34 (2008); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOMELAND SEC., OIG-09-109, EVALUATION OF DHS' INFORMATION SECURITY PROGRAM FOR FY 2009 12- 13 (2009); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOMELAND SEC., OIG 11-01, EVALUATION OF DHS' INFORMATION SECURITY PROGRAM FOR FY 2010 12 (2010); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOMELAND SEC., OIG 11-113, EVALUATION OF DHS' INFORMATION SECURITY PROGRAM FOR FY 2011 1 (2011); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOMELAND SEC., OIG 13-04, EVALUATION OF DHS' INFORMATION SECURITY PROGRAM FOR FY 2012 13 (2012); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOMELAND SEC., OIG 14-09, EVALUATION OF DHS' INFORMATION SECURITY PROGRAM FOR FY 2013 5 (2013); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOMELAND SEC., OIG 15-16, EVALUATION OF DHS' INFORMATION SECURITY PROGRAM FOR FY 2014 18 (2014); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOMELAND SEC., OIG 16-08, EVALUATION OF DHS' INFORMATION SECURITY PROGRAM FOR FY 2015 21 (2016); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOMELAND SEC., OIG 17-24, EVALUATION OF DHS' INFORMATION SECURITY PROGRAM FOR FY 2016, DHS OIG HIGHLIGHTS 12 (2017); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOMELAND SEC., OIG 18- 56, EVALUATION OF DHS' INFORMATION SECURITY PROGRAM FOR FY 2017 10 (2018); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOMELAND SEC., OIG 19-60, EVALUATION OF DHS' INFORMATION SECURITY PROGRAM FOR FY 2018 15 (2018); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOMELAND SEC., OIG 20-77, EVALUATION OF DHS' INFORMATION SECURITY PROGRAM FOR FY 2019 22 (2020).
[149] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOMELAND SEC., OIG 20-77, EVALUATION OF DHS' INFORMATION SECURITY PROGRAM FOR FY 2019 7 (2020).

inventory of its information systems, including high value assets."[150] High value assets are systems containing sensitive data used for critical agency operations or otherwise containing data that would be of particular interest to hostile actors.[151]

B. The State Department

The State Department (State) aims to advance the national interests of the United States and its people.[152] The Department executes this mission by leading "America's foreign policy through diplomacy, advocacy, and assistance."[153]

As the lead agency for American foreign policy, State has a wealth of both PII and sensitive national security information. For example, State's Consular Consolidated Database (CCD) maintains "current and archived data from all of the Consular Affairs post databases around the world."[154] This data includes PII like names, birthdates, and Social Security numbers used for visa and passport vetting.[155] On the national security side, State's Blue Lantern program "monitors the end-use of defense articles, technical data, defense services, and brokering activities exported through commercial channels . . . ."[156] The program is designed to minimize misappropriation of U.S. defense articles and ensure such articles and services are used for their intended purpose.[157]

The State Department's information security program received an overall Level 2, "Defined" maturity rating, [158] effectively a D. State was ineffective in four of five function areas including a Level 1, "Ad-hoc" maturity rating for detection capabilities.[159] This is the lowest possible rating within the Federal Government's maturity model.[160]

Lack of Valid Authorities to Operate. Auditors identified many State Department systems operating without current authorizations. For example, of the 487 systems on the Department's network, 128 (or 26 percent) did not have valid authorizations.[161] These weaknesses

---

[150] *Id.* at 9.
[151] *Id.* at 16 n.19.
[152] *About the U.S. Department of State – Our Mission*, U.S. Dep't of State, https://www.state.gov/about/about-the-u-s-department-of-state/.
[153] *Id.*
[154] U.S. DEP'T OF STATE, CONSULAR CONSOLIDATED DATABASE PRIVACY IMPACT ASSESSMENT 1 (2018).
[155] *Id.* at 3.
[156] U.S. DEP'T OF STATE, REPORT TO CONGRESS ON THE END-USE MONITORING OF DEFENSE ARTICLES AND DEFENSE SERVICES 1 (2019).
[157] *Id.* at 1−2.
[158] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF STATE, AUD-IT-21-25, AUDIT OF THE DEPARTMENT OF STATE FY 2020 INFORMATION SECURITY PROGRAM 5 (2021).
[159] *Id.*
[160] *Id.* at 4.
[161] *Id.* at 19.

demonstrate that "the Department did not perform timely, required security assessments."[162] The Inspector General also identified this issue in FY 2015.[163]

Use of Unsupported Systems. The State Department Inspector General found State uses systems that are no longer supported by the vendor.[164] Of the ten systems tested by auditors, vulnerability scans identified two kinds of software no longer supported by the vendor—including an unsupported version Microsoft Windows.[165] Moreover, "the Department did not have a software lifecycle management process to manage the end of life for unsupported software on its network."[166]

Failure to Remediate Vulnerabilities. The State Department failed to remediate vulnerabilities in a timely fashion. Tests of 10 Department systems revealed 450 critical-risk and 736 high-risk outstanding vulnerabilities.[167] Criticality describes "the degree to which an organization depends on the information or information system for the success of a mission or of a business function."[168] This number of outstanding vulnerabilities demonstrates the Department's failure to comply with its own policy for patch management and vulnerability remediation.[169]

Tests of 10 Department systems revealed 450 critical-risk and 736 high-risk outstanding vulnerabilities.

The Inspector General also found an alarming number of security vulnerabilities with the State Department's user management. For example, State Department was not able to provide documentation of user access agreements for 60 percent of the sample employees tested with access to the Department's classified network.[170] This network contains data which if disclosed to an unauthorized person could cause "grave damage" to national security.[171] Perhaps more troubling, State failed to shut off thousands of accounts after extended periods of inactivity on both its classified and sensitive but unclassified networks.[172] According to the Inspector General, some accounts remained active as long as 152 days after employees quit, retired, or were fired.[173] Former employees or hackers could use those unexpired credentials to gain access to State's sensitive and classified information, while appearing to be an authorized user.[174] The

[162] *Id.* at 19−20.
[163] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF STATE, AUD-IT-16-16, AUDIT OF DEPARTMENT OF STATE INFORMATION SECURITY PROGRAM 10 (2015).
[164] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF STATE, AUD-IT-21-25, AUDIT OF THE DEPARTMENT OF STATE FY 2020 INFORMATION SECURITY PROGRAM 9 (2021).
[165] *Id.*
[166] *Id.* at 25.
[167] *Id.* at 9.
[168] *Criticality*, NIST COMPUTER SEC. RESOURCE CENTER GLOSSARY, https://csrc nist.gov/glossary/term/criticality.
[169] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF STATE, AUD-IT-21-25, AUDIT OF THE DEPARTMENT OF STATE FY 2020 INFORMATION SECURITY PROGRAM 9 (2021).
[170] *Id.* at 12.
[171] Exec. Order No. 13526, 75 Fed. Reg. 707, § 1.1(b) (Jan. 5, 2010).
[172] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF STATE, AUD-IT-21-25, AUDIT OF THE DEPARTMENT OF STATE FY 2020 INFORMATION SECURITY PROGRAM 12 (2021).
[173] *Id.*
[174] *Id.*

Inspector General warned that without resolving issues in this category, "the risk of unauthorized access is significantly increased."[175]

When the Inspector General recommended State ensure accounts unused for more than 60 days are disabled as required by State policies, State disagreed, apparently citing a memorandum regarding another matter entirely—the requirement that users change their password every 90 days.[176] The Inspector General responded saying State's IT office "may not understand the intent of the recommendation."[177]

This was not the only example in which State seemed to misunderstand a recommendation by the Inspector General. The State Inspector General also found that some agency employees only had access to the classified network at State.[178] This meant that they could not access or take the required training on IT security which was hosted only on State's the unclassified network.[179] As a result, the Inspector General recommended State ensure that employees with access to its classified network access also be given access the IT security training.[180] In response, State objected writing, "sufficient training exists to inform individuals about how to work with and handle classified information."[181] Yet the recommendation related to training on IT security, not handling of classified information.[182] The Inspector General responded again saying State's IT office "may not understand the intent of the recommendation."[183]

The Inspector General also cited State's failure to remediate vulnerabilities in FY 2015, 2016, and 2018.[184]

Failure to Compile an Accurate and Comprehensive IT Asset Inventory. The State Department failed to "maintain a comprehensive, accurate, and up-to-date inventory list of IT hardware and software components, nor did it adequately manage software licenses."[185] While the Department provided the number of devices on its network, it "could not provide a complete inventory of hardware."[186] In response to these findings, State explained its network management tools "do

[175] *Id.* at 26.
[176] *Id.* at 13, 44, 46–47, 51.
[177] *Id.* at 13.
[178] *Id.* at 17.
[179] *Id.*
[180] Although the final recommendation was re-worded for clarity, OFFICE OF INSPECTOR GENERAL, U.S. DEP'T OF STATE, AUD-IT-21-25, AUDIT OF THE DEPARTMENT OF STATE FY 2020 INFORMATION SECURITY PROGRAM 18 (2021), the earlier version still clearly related to training for IT security not protection and handling of classified information, recommending that State "complete its effort to develop and implement IT security training that is specific to [its classified network]." *Id.* at 47.
[181] *Id.* at 18.
[182] *Id.*
[183] *Id.*
[184] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF STATE, AUD-IT-16-16, AUDIT OF DEPARTMENT OF STATE INFORMATION SECURITY PROGRAM 16 (2015); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF STATE, AUD-IT-17-17, AUDIT OF THE DEPARTMENT OF STATE INFORMATION SECURITY PROGRAM 11 (2016); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF STATE, AUD-IT-19-08, AUDIT OF THE DEPARTMENT OF STATE INFORMATION SECURITY PROGRAM 12 (2018).
[185] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF STATE, AUD-IT-21-25, AUDIT OF THE DEPARTMENT OF STATE FY 2020 INFORMATION SECURITY PROGRAM 5 (2021).
[186] *Id.*

not provide information on location, asset owner, and related information system."[187] The Inspector General also flagged this issue in FY 2016, 2017, and 2018.[188]

Failure to Provide for the Adequate Protection of PII. Auditors identified weaknesses related to State's protection of sensitive information and noted the Department "did not have an effective data protection and privacy program in place."[189] Moreover, State was unable to "document that it had defined controls related to the protection of data at rest and in transit."[190] The Inspector General also cited State for this issue in FY 2016, 2017, and 2018.[191]

C. The Department of Transportation

The Department of Transportation (DOT) seeks to ensure the "safest, most efficient and modern transportation system in the world, which boosts [American] economic productivity and global competitiveness and enhances the quality of life in communities both rural and urban."[192]

An example of a DOT database containing PII is the National Highway Traffic Safety Administration's (NHTSA) Artemis system.[193] Artemis collects PII including names, email, telephone numbers, addresses, and vehicle information so NHTSA can process consumer complaints and conduct recall investigations.[194] DOT also includes the Federal Aviation Administration, which operates our nation's commercial air traffic control system, instructing planes where to fly and where and when to land.[195]

---

[187] *Id.* at 5–6.
[188] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF STATE, AUD-IT-17-17, AUDIT OF THE DEPARTMENT OF STATE INFORMATION SECURITY PROGRAM 8 (2016); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF STATE, AUD-IT-18-12, AUDIT OF THE DEPARTMENT OF STATE INFORMATION SECURITY PROGRAM 7–8 (2017); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF STATE, AUD-IT-19-08, AUDIT OF THE DEPARTMENT OF STATE INFORMATION SECURITY PROGRAM 8 (2018).
[189] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF STATE, AUD-IT-21-25, AUDIT OF THE DEPARTMENT OF STATE FY 2020 INFORMATION SECURITY PROGRAM 14 (APR. 2021).
[190] *Id.* at 15.
[191] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF STATE, AUD-IT-17-17, AUDIT OF THE DEPARTMENT OF STATE INFORMATION SECURITY PROGRAM 19 (2016); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF STATE, AUD-IT-18-12, AUDIT OF THE DEPARTMENT OF STATE INFORMATION SECURITY PROGRAM 22 (2017); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF STATE, AUD-IT-19-08, AUDIT OF THE DEPARTMENT OF STATE INFORMATION SECURITY PROGRAM 23 (2018).
[192] *What We Do,* U.S. DEP'T OF TRANSP., https://www.transportation.gov/about.
[193] U.S. DEP'T OF TRANSP., PRIVACY IMPACT ASSESSMENT NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION ARTEMIS 1 (2015).
[194] *Id.* at *1*–2.
[195] *Air Traffic*, FED. AVIATION ADMIN., U.S. DEP'T OF TRANSP., https://www.faa.gov/air_traffic/.

DOT's information security program was ineffective in all five NIST function areas.[196] DOT's overall program received a Level 2, "Defined," maturity rating—"the second lowest level in the maturity model for an information security program,"[197] tantamount to a D.

As the Inspector General cautioned in its report, "DOT relies on hundreds of information systems to carry out its missions, including safe air traffic control operations, and handling billions of taxpayer dollars" for "major transportation projects, such as highway construction and high-speed rail development."[198] The maintenance of DOT systems costs roughly $3.6 billion per year—"one of the largest IT investments among Federal civilian agencies."[199] DOT needs to implement policies and practices to "protect these systems from malicious attacks and other compromises that may put citizen safety or taxpayer dollars at risk."[200]

Lack of Valid Authorities to Operate. Expired authorizations have long plagued DOT. During its review, the DOT Inspector General found the Department operates systems with expired authorizations.[201] Of the 63 systems reviewed by the Inspector General, 33 had authorizations that were "expired, authorized with the incorrect risk representation, not authorized by the appropriate Authorizing Official, or not provided."[202] Based on this analysis, the Inspector General estimates 250 of 430, or 58.2 percent, of total department systems currently lack valid authorizations.[203] This is a significant increase from the 61 systems operating without authorizations at the time of the Subcommittee's report in 2019.[204] Without confirmation that security controls are operating as intended, DOT is vulnerable to "information loss, fraud, or abuse."[205] The DOT Inspector General cited DOT for this issue for the last *eleven* consecutive fiscal years.[206]

---

[196] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF TRANSP., REPORT NO. QC2021003, U.S. DEPARTMENT OF TRANSPORTATION'S 2020 FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 AUDIT 2 (2020).
[197] *Id.* at 1.
[198] *Id.* at 24, 26.
[199] *Id.* at 26.
[200] *Id.* at 24.
[201] *Id.* at 8.
[202] *Id.*
[203] *Id.*
[204] STAFF OF S. PERMANENT SUBCOMM. ON INVESTIGATIONS, 116TH CONG., REP. ON FEDERAL CYBERSECURITY: AMERICA'S DATA AT RISK 52 (2019); Office of Inspector General, U.S. Dep't of Transportation, Report No. QC2021003, U.S. Department of Transportation's 2020 Federal Information Security Modernization Act of 2014 Audit, 8 (Oct. 9, 2020).
[205] *Id.*
[206] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF TRANSP., REPORT NO. FI2011022, TIMELY ACTIONS NEEDED TO IMPROVE DOT'S CYBERSECURITY 17 (2010); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF TRANSP., REPORT NO. FI2012007, FISMA 2011: PERSISTENT WEAKNESSES IN DOT'S CONTROLS CHALLENGE THE PROTECTION AND SECURITY OF ITS INFORMATION SYSTEMS 12 (2011); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF TRANSP., REPORT NO. FI2013014, FISMA 2012: ONGOING WEAKNESSES IMPEDE DOT'S PROGRESS TOWARD EFFECTIVE INFORMATION SECURITY 12 (2012); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF TRANSP., REPORT NO. FI2014006, FISMA 2013: DOT HAS MADE PROGRESS, BUT ITS SYSTEMS REMAIN VULNERABLE TO SIGNIFICANT SECURITY THREATS 13 (2013); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF TRANSP., REPORT NO. FI2015009, FISMA 2014: DOT HAS MADE PROGRESS BUT SIGNIFICANT WEAKNESSES IN ITS INFORMATION SECURITY REMAIN 15 (2014); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF TRANSP., REPORT NO. FI2016001, FISMA 2015: DOT HAS MAJOR SUCCESS IN PIV IMPLEMENTATION, BUT PROBLEMS PERSIST IN OTHER CYBERSECURITY AREAS 21 (2015); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF TRANSP., REPORT NO. FI2017008, FISMA 2016: DOT CONTINUES TO MAKE PROGRESS, BUT

Use of Unsupported Systems. The DOT Inspector General's review identified six systems of a 63-system sample using unsupported software.[207] These unsupported systems included Windows 2008, which Microsoft stopped supporting five years ago.[208]

The DOT Inspector General consistently cited the Department for using unsupported software. For example, in FY 2018, the Inspector General found the Department was using Windows 2003 servers no longer supported by Microsoft.[209] In FY 2017, the Inspector General identified the similar use of an unsupported Adobe Acrobat product.[210]

Failure to Remediate Vulnerabilities. Eighty-seven percent of systems reviewed by the Inspector General had ineffective "baseline compliance monitoring [or] vulnerability management processes."[211] Moreover, the Inspector General determined 60 percent of sampled systems had ineffective patch management processes.[212] Finally, 37 percent of reviewed systems failed to remediate critical vulnerabilities within the timeframe established by the Department.[213] These vulnerability management weaknesses could result in "potential harm to data confidentiality, integrity, and availability."[214]

The DOT Inspector General also determined the Department does not enforce OMB's configuration management requirements.[215] In particular, DOT has not fully implemented configuration management controls "designed to ensure DOT's critical systems have appropriate security baselines, current and vendor supported operating systems, accurate system and software inventories, and up-to-date vulnerability patches."[216] DOT has policies requiring these controls, but the Department "has not consistently implemented vulnerability remediation and management processes."[217]

THE DEPARTMENT'S INFORMATION SECURITY POSTURE IS STILL NOT EFFECTIVE 8 (2016); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF TRANSP., REPORT NO. FI2018017, FISMA 2017: DOT'S INFORMATION SECURITY POSTURE IS STILL NOT EFFECTIVE 9−10 (2018); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF TRANSP., REPORT NO. FI2019023, FISMA 2018: DOT'S INFORMATION SECURITY PROGRAM AND PRACTICES 6 (2019); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF TRANSP., REPORT NO. QC2020002, U.S. DEPARTMENT OF TRANSPORTATION'S 2019 FEDERAL INFORMATION SECURITY MODERNIZATION ACT (FISMA) AUDIT 12−13 (2019); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF TRANSP., REPORT NO. QC2021003, U.S. DEPARTMENT OF TRANSPORTATION'S 2020 FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 AUDIT 7−9 (2020).

[207] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF TRANSP., REPORT NO. QC2021003, U.S. DEPARTMENT OF TRANSPORTATION'S 2020 FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 AUDIT 11 (2020).

[208] *Id.*; *Windows 8 end of support and Office*, MICROSOFT (Jan. 12, 2016), https://support.microsoft.com/en-us/office/windows-8-end-of-support-and-office-34e28be4-1e4f-4928-b210-3f45d8215595.

[209] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF TRANSP., REPORT NO. FI2019023, FISMA 2018: DOT'S INFORMATION SECURITY PROGRAM AND PRACTICES 45 (2019).

[210] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF TRANSP., REPORT NO. FI2018017, FISMA 2017: DOT'S INFORMATION SECURITY POSTURE IS STILL NOT EFFECTIVE 52 (2018).

[211] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF TRANSP., REPORT NO. QC2021003, U.S. DEPARTMENT OF TRANSPORTATION'S 2020 FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 AUDIT 11 (2020).

[212] *Id.*

[213] *Id.*

[214] *Id.* at 12.

[215] *Id.* at 11 (citing OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, M-14-03, ENHANCING THE SECURITY OF FEDERAL INFORMATION AND INFORMATION SYSTEMS (2013)).

[216] *Id.* at 11.

[217] *Id.*

The Inspector General's finding regarding ineffective vulnerability management is not new. In FY 2018, DOT failed to install patches for 86 critical, 203 high, and 352 medium vulnerabilities.[218] Although the Department developed a patching plan following the 2018 audit, DOT still struggles to implement patches within its designated timeframe.[219] This gives adversaries more time to exploit these vulnerabilities. Like a window left open at home, the longer it is left open and unattended, the more likely that a burglar climbs in and steals everything.

The Inspector General found the Department's hardware inventory failed to account for 14,935 assets.

Failure to Compile an Accurate and Comprehensive IT Asset Inventory. DOT lacks accurate IT system and asset inventories.[220] For example, the Inspector General found the Department's hardware inventory failed to account for 14,935 assets.[221] These unaccounted assets included 7,231 mobile devices, 4,824 servers, and 2,880 workstations.[222] Due to these weaknesses, DOT "may not be aware of all assets residing in its environment and therefore may not be appropriately managing and protecting all assets."[223]

The Inspector General cited DOT's lack of accurate inventories in *every* fiscal year since 2008.[224] The Department did, however, make a substantial improvement—reducing the total

---

[218] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF TRANSP., REPORT NO. FI2019023, FISMA 2018: DOT'S INFORMATION SECURITY PROGRAM AND PRACTICES 44 (2019).
[219] *Id.*; OFFICE OF INSPECTOR GEN., U.S. DEP'T OF TRANSP., REPORT NO. QC2021003, U.S. DEPARTMENT OF TRANSPORTATION'S 2020 FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 AUDIT 11 (2020).
[220] *Id.* at 9.
[221] *Id.* at 10.
[222] *Id.*
[223] *Id.*
[224] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF TRANSP., REPORT NO. FI2009003, AUDIT OF INFORMATION SECURITY PROGRAM 4 (2008); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF TRANSP., REPORT NO. FI2010023, AUDIT OF DOT'S INFORMATION SECURITY PROGRAM AND PRACTICES 3 (2009); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF TRANSP., REPORT NO. FI2011022, TIMELY ACTIONS NEEDED TO IMPROVE DOT'S CYBERSECURITY 14 (2010); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF TRANSP., REPORT NO. FI2012007, FISMA 2011: PERSISTENT WEAKNESSES IN DOT'S CONTROLS CHALLENGE THE PROTECTION AND SECURITY OF ITS INFORMATION SYSTEMS 19 (2011); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF TRANSP., REPORT NO. FI2013014, FISMA 2012: ONGOING WEAKNESSES IMPEDE DOT'S PROGRESS TOWARD EFFECTIVE INFORMATION SECURITY 7−8 (2012); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF TRANSP., REPORT NO. FI2014006, FISMA 2013: DOT HAS MADE PROGRESS, BUT ITS SYSTEMS REMAIN VULNERABLE TO SIGNIFICANT SECURITY THREATS 8 (2013); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF TRANSP., REPORT NO. FI-2015-009, FISMA 2014: DOT HAS MADE PROGRESS BUT SIGNIFICANT WEAKNESSES IN ITS INFORMATION SECURITY REMAIN 24–25 (2014); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF TRANSP., REPORT NO. FI2016001, FISMA 2015: DOT HAS MAJOR SUCCESS IN PIV IMPLEMENTATION, BUT PROBLEMS PERSIST IN OTHER CYBERSECURITY AREAS 15 (2015); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF TRANSP., REPORT NO. FI2017008, FISMA 2016: DOT CONTINUES TO MAKE PROGRESS, BUT THE DEPARTMENT'S INFORMATION SECURITY POSTURE IS STILL NOT EFFECTIVE 11 (2016); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF TRANSP., REPORT NO. FI2018017, FISMA 2017: DOT'S INFORMATION SECURITY POSTURE IS STILL NOT EFFECTIVE 13−14 (2018); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF TRANSP., REPORT NO. FI2019023, FISMA 2018: DOT'S INFORMATION SECURITY PROGRAM AND PRACTICES 44 (2019); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF TRANSP., REPORT NO. QC2020002, U.S. DEPARTMENT OF TRANSPORTATION'S 2019 FEDERAL INFORMATION SECURITY MODERNIZATION ACT (FISMA) AUDIT 14 (2019); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF TRANSP., REPORT NO. QC2021003, U.S. DEPARTMENT OF TRANSPORTATION'S 2020 FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 AUDIT 9 (2020).

unaccounted for assets by over 54 percent—from FY 2019 when the Inspector General found 32,814 assets not properly accounted for in DOT inventories.[225]

Failure to Provide for the Adequate Protection of PII. OMB guidance from 2012 requires federal agencies to use personal identity verification (PIV) cards to access agency computers as part of multifactor authentication.[226] PIV card use strengthens network access security by requiring "a computer system user to authenticate his or her identity by at least two unique factors."[227] Despite this requirement, 203 DOT systems are not configured to enable PIV card use or a comparable method of multifactor authentication.[228] In addition, approximately 41 percent of systems containing PII also did not require PIV authentication.[229] Without a waiver, the *Federal Cybersecurity Enhancement Act of 2015* requires multifactor authentication, such as PIV authentication, for remote access and privileged accounts.[230]

In the two years since the Subcommittee's report, DOT equipped 8 systems with PIV card use down from 211 systems without this capability.[231] Over that same timeframe, PII systems not requiring PIV card authentication grew by 27—up to 81 from 54.[232] Multifactor authentication like a PIV card makes it more difficult for a hacker to logon to an information system and gain access to sensitive data on it, even if they have a stolen password from the user. By not using multi-factor authentication consistently, agencies make it easier for a hacker to use stolen credentials to get on a network, access data, and establish persistence.

D. The Department of Housing and Urban Development

The Department of Housing and Urban Development (HUD) seeks "to create strong, sustainable, inclusive communities and quality affordable homes for all."[233] HUD also works to "strengthen the housing market to bolster the economy and protect consumers [and] utilize housing as a platform for improving quality of life . . . ."[234]

HUD has a significant number of PII databases including the Tenant Rental Assistance Certification System (TRACS) and the Enterprise Income Verification (EIV) system. HUD maintains "at least a billion records containing the personally identifiable information (PII) of

---

[225] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF TRANSP., REPORT NO. QC2020002, U.S. DEPARTMENT OF TRANSPORTATION'S 2019 FEDERAL INFORMATION SECURITY MODERNIZATION ACT (FISMA) AUDIT 14 (2019).
[226] *Id.* at 13.
[227] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF TRANSP., REPORT NO. FI2019023, FISMA 2018: DOT'S INFORMATION SECURITY PROGRAM AND PRACTICES 19 (2019).
[228] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF TRANSP., REPORT NO. QC2021003, U.S. DEPARTMENT OF TRANSPORTATION'S 2020 FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 AUDIT 14 (2020).
[229] *Id.*
[230] Consolidated Appropriations Act, Pub. L. No. 114-113 § 225, Title II, Subtitle B−Federal Cybersecurity Enhancement Act, 129 Stat. 2967 (2015), 6 U.S.C. § 1501. *See also supra* Part III. C.
[231] STAFF OF S. PERMANENT SUBCOMM. ON INVESTIGATIONS, 116TH CONG., REP. ON FEDERAL CYBERSECURITY: AMERICA'S DATA AT RISK 53 (2019).
[232] *Id.*; OFFICE OF INSPECTOR GEN., U.S. DEP'T OF TRANSP., REPORT NO. QC2021003, U.S. DEPARTMENT OF TRANSPORTATION'S 2020 FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 AUDIT 14 (2020).
[233] *Mission*, U.S. DEP'T OF HOUS. & URBAN DEV., https://www.hud.gov/about/mission.
[234] *Id.*

American citizens and facilitate[s] thousands of transactions with business partners and private individuals daily."[235] These databases include sensitive information on one of the most vulnerable populations of Americans. HUD uses PII including names, addresses, income, and employment history to confirm tenant eligibility for assisted housing programs.[236] The EIV system then pulls from this same TRACS data to confirm "the right rental assistance benefits go to the right persons."[237]

The HUD Inspector General determined the Department improved its overall maturity to Level 3, "Consistently Implemented," for FY 2020, [238] an effective grade of C. Although HUD's information security program is not yet effective under FISMA, the FY 2020 evaluation is HUD's highest rating ever and noted the CIO's "significant accomplishments."[239] HUD also closed 29 Inspector General recommendations, "more than 4 times the number closed in FY 2019."[240] Despite these notable improvements, 79 Inspector General recommendations remain open.[241]

Lack of Valid Authorities to Operate. HUD did not always follow system security principles "and shadow IT existed without approved authorities to operate."[242] Shadow IT refers to "IT-related hardware, software or cloud services [used] without the knowledge of the IT organization."[243] To address these weaknesses, HUD has attempted to enhance controls over their IT environment and ensure appropriate security controls are implemented.[244]

The Inspector General also flagged this weakness in FY 2018 when it determined HUD's official website lacked proper authorization.[245] Reducing shadow IT is critical because "IT staff may not learn of the existence of [a] system until it fails or is breached, jeopardizing the critical mission."[246] Because IT staff do not know these systems exist, security controls are not validated, and they can remain unpatched introducing security vulnerabilities into the HUD environment.

Use of Unsupported Systems. Legacy IT continues to be a significant challenge for HUD. The Inspector General made clear that Department's IT environment—which is mostly composed of legacy systems—"makes HUD's networks and information technology (IT) resources

---

[235] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOUS. & URBAN DEV., 2020-OE-0001, HUD FISCAL YEAR 2020 FEDERAL INFORMATION SECURITY MODERNIZATION ACT 2014 EVALUATION REPORT 5 (2020).
[236] U.S. DEP'T OF HOUS. & URBAN DEV., TENANT RENTAL ASSISTANCE CERTIFICATION SYSTEM PRIVACY IMPACT ASSESSMENT 7–8 (2009).
[237] U.S. DEP'T OF HOUS. & URBAN DEV., ENTERPRISE INCOME VERIFICATION SYSTEM PRIVACY IMPACT ASSESSMENT 2 (2017).
[238] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOUS. & URBAN DEV., 2020-OE-0001, HUD FISCAL YEAR 2020 FEDERAL INFORMATION SECURITY MODERNIZATION ACT 2014 EVALUATION REPORT 2 (2020).
[239] *Id.*
[240] *Id.* at 11−12.
[241] *Id.* at 11.
[242] *Id.* at 15.
[243] *Id.* at n.16.
[244] *Id.* at 35.
[245] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOUS. & URBAN DEV., 2018-OE-0003, HUD FISCAL YEAR 2018 FEDERAL INFORMATION SECURITY MODERNIZATION ACT 2014 EVALUATION REPORT 10 (2018).
[246] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOUS. & URBAN DEV., 2020-OE-0001, HUD FISCAL YEAR 2020 FEDERAL INFORMATION SECURITY MODERNIZATION ACT 2014 EVALUATION REPORT 15 n.16 (2020).

susceptible to malicious activity and exploitation."[247] This is of particular concern for HUD's mission-essential applications, many of which "have not been modernized in decades."[248] Some of these applications are mainframe platforms "which are operationally inefficient, increasingly difficult to secure, and costly to maintain."[249] For example, in 2015, Chinese-attributed hackers gained access to legacy mainframes at the Office of Personnel Management to steal sensitive data on 21.5 million current and former Federal employees.[250]

As a longstanding issue at the Department, HUD previously reported using the majority of its information security budget on the maintenance of legacy systems.[251] The Inspector General noted HUD's overreliance on these outdated systems in every annual evaluation since FY 2013.[252]

The Inspector General made clear that Department's IT environment—which is mostly composed of legacy systems—"makes HUD's networks and information technology (IT) resources susceptible to malicious activity and exploitation." This is of particular concern for HUD's mission-essential applications, many of which "have not been modernized in decades."

Failure to Compile Accurate and Comprehensive IT Asset Inventory. HUD maintains an inventory of systems operating on its network, but the Department "continues to face the challenge of identifying and ensuring that all

[247] *Id.* at 2, 5.
[248] *Id.* at 5.
[249] *Id.*
[250] Press Release, Office of Personnel Management, Statement by OPM Press Secretary Sam Schumach on Background Investigations Incident (Sept. 23, 2015), https://www.opm.gov/news/releases/2015/09/cyber-statement-923/; *OPM: Data Breach Hearing Before the H. Comm. on Oversight and Gov't Reform*, 114th Cong. 43 (2015) (testimony of Katherine Archuleta, Director, Office of Personnel Management); Devlin Barrett, *Chinese national arrested for allegedly using malware linked to OPM hack*, WASH. POST (Aug. 24, 2017), https://www.washingtonpost.com/world/national-security/chinese-national-arrested-for-using-malware-linked-to-opm-hack/2017/08/24/746cbdc2-8931-11e7-a50f-e0d4e6ec070a_story html.
[251] STAFF OF S. PERMANENT SUBCOMM. ON INVESTIGATIONS, 116TH CONG., REP. ON FEDERAL CYBERSECURITY: AMERICA'S DATA AT RISK 60 (2019).
[252] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOUS. & URBAN DEV., 2013-ITED-0001, FEDERAL INFORMATION SECURITY MANAGEMENT ACT FISCAL YEAR 2013 EVALUATION REPORT 6, 10, 18 (2013); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOUS. & URBAN DEV., 2014-OE-0003, FEDERAL INFORMATION SECURITY MANAGEMENT ACT FISCAL YEAR 2014 EVALUATION REPORT 3 (2014); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOUS. & URBAN DEV., 2015-OE-0001, HUD FISCAL YEAR 2015 FISMA EVALUATION REPORT 31 (2015); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOUS.& URBAN DEV., 2016-OE-0006, HUD FISCAL YEAR 2016 FEDERAL INFORMATION SECURITY MODERNIZATION ACT 2014 EVALUATION REPORT 32 (2016); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOUS. & URBAN DEV., 2017-OE-0007, HUD FISCAL YEAR 2017 FEDERAL INFORMATION SECURITY MODERNIZATION ACT 2014 EVALUATION REPORT 5 (2017); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOUS. & URBAN DEV., 2018-OE-0003, HUD FISCAL YEAR 2018 FEDERAL INFORMATION SECURITY MODERNIZATION ACT 2014 EVALUATION REPORT 4 (2018); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOUS. & URBAN DEV., 2019-OE-0002, HUD FISCAL YEAR 2019 FEDERAL INFORMATION SECURITY MODERNIZATION ACT 2014 EVALUATION REPORT 2 (2020); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOUS. & URBAN DEV., 2020-OE-0001, HUD FISCAL YEAR 2020 FEDERAL INFORMATION SECURITY MODERNIZATION ACT 2014 EVALUATION REPORT 5 (2020).

systems, particularly web applications, are included in system inventory."[253] For example, the Inspector General identified "over a dozen web applications containing HUD data that were not using HUD's primary web address or the required government domain name."[254] Many of the addresses discovered during the Inspector General's evaluation were not documented in HUD's web application inventory.[255] The Inspector General also found HUD program offices failed to adhere to the Department's policy for conducting annual scans of their systems.[256] For instance, "one sample system assessed during [the] evaluation had not been scanned in 4 years."[257]

The Department's challenges with system inventory management date back to at least FY 2008.[258] To resolve this issue, the Inspector General recommended HUD "implement a software asset management capability for software and operating systems to ensure that software executes only from the authorized software inventory."[259]

Failure to Provide for the Adequate Protection of PII. Several HUD systems that process, store, or transmit PII did not require multifactor authentication of nonprivileged or privileged users.[260] As noted earlier, the *Federal Cybersecurity Enhancement Act of 2015* generally requires multifactor authentication be in place for privileged users absent a waiver.[261] In addition, HUD "did not maintain an inventory of the collection and use of all PII or have a process for reviewing and limiting the collection of PII."[262] Efforts to compile such an inventory were complicated by program offices' lack of awareness regarding "the amount and location of PII under their purview."[263] This lack of awareness was partially attributed to program offices' differing interpretations of what information constituted PII.[264] The Inspector General noted weaknesses in this area for the last *eight* consecutive years.[265]

---

[253] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOUS. & URBAN DEV., 2020-OE-0001, HUD FISCAL YEAR 2020 FEDERAL INFORMATION SECURITY MODERNIZATION ACT 2014 EVALUATION REPORT 14 (2020).
[254] *Id.* at 43.
[255] *Id.*
[256] *Id.* at 19.
[257] *Id.*
[258] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOUS. & URBAN DEV., MEMORANDUM NO. 2008-DP-0802, OIG RESPONSE TO QUESTIONS FROM OMB UNDER THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002 3 (2008).
[259] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOUS. & URBAN DEV., 2020-OE-0001, HUD FISCAL YEAR 2020 FEDERAL INFORMATION SECURITY MODERNIZATION ACT 2014 EVALUATION REPORT 16 (2020).
[260] *Id.* at 23.
[261] Consolidated Appropriations Act, Pub. L. No. 114-113 § 225, Title II, Subtitle B−Federal Cybersecurity Enhancement Act, 129 Stat. 2967 (2015), 6 U.S.C. § 1501. *See also supra* Part III. C.
[262] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOUS. & URBAN DEV., 2020-OE-0001, HUD FISCAL YEAR 2020 FEDERAL INFORMATION SECURITY MODERNIZATION ACT 2014 EVALUATION REPORT 26 (2020).
[263] *Id.* at 27.
[264] *Id.*
[265] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOUS. & URBAN DEV., 2013-ITED-0001, FEDERAL INFORMATION SECURITY MANAGEMENT ACT FISCAL YEAR 2013 EVALUATION REPORT 9 (2013); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOUS. & URBAN DEV., 2014-OE-0003, FEDERAL INFORMATION SECURITY MANAGEMENT ACT FISCAL YEAR 2014 EVALUATION REPORT 23, 36 (2014); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOUS.& URBAN DEV., 2015-OE-0001, HUD FISCAL YEAR 2015 FISMA EVALUATION REPORT 1, 15 (2015); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOUS. & URBAN DEV., 2016-OE-0006, HUD FISCAL YEAR 2016 FEDERAL INFORMATION SECURITY MODERNIZATION ACT 2014 EVALUATION REPORT 40−41, 47 (2016); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOUS. & URBAN DEV., 2017-OE-0007, HUD FISCAL YEAR 2017 FEDERAL INFORMATION SECURITY

E. The Department of Agriculture

The Department of Agriculture (USDA) works "to provide economic opportunity through innovation helping rural America to thrive; to promote agriculture production that better nourishes Americans while also helping feed others throughout the world; and to preserve our Nation's natural resources through conservation, restored forests, improved watersheds, and healthy private working lands."[266]

USDA maintains several repositories of sensitive information. The Department's Direct Loan System (DLS) stores PII including names, Social Security numbers, liabilities, and assets owned to process loan applications.[267] USDA's Supplemental Nutrition Assistance Program (SNAP) "provides nutrition benefits to supplement the food budget of needy families."[268] USDA also has sensitive national security information related to its participation in the Select Agent Program and the Food Safety and Inspection Service's vulnerability assessments. As part of the Select Agent Program, USDA oversees and regulates hazardous toxins that could threaten animal or plant products.[269] The Food Safety and Inspection Service's vulnerability assessments "inform the development of countermeasures to help prevent or mitigate the impacts of an intentional attack on the food supply."[270]

USDA's rating improved to a Level 3, "Consistently Implemented" maturity level, [271] effectively a grade of C. While the Department's rating improved, its information security program is still ineffective under FISMA.[272] As a decentralized agency with many functions, USDA "does not have an organization-wide view of the many IT processes and controls."[273]

Use of Unsupported Systems. As was the case in previous audits, the Inspector General again identified USDA's use of unsupported software.[274] Using this software exposes USDA to risks

---

MODERNIZATION ACT 2014 EVALUATION REPORT 30−31, 36 (2017); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOUS. & URBAN DEV., 2018-OE-0003, HUD FISCAL YEAR 2018 FEDERAL INFORMATION SECURITY MODERNIZATION ACT 2014 EVALUATION REPORT 21 (2018); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOUS. & URBAN DEV., 2019-OE-0002, HUD FISCAL YEAR 2019 FEDERAL INFORMATION SECURITY MODERNIZATION ACT 2014 EVALUATION REPORT 19 (2020); OFFICE OF INSPECTOR GEN, U.S. DEP'T OF HOUS.& URBAN DEV., 2020-OE-0001, HUD FISCAL YEAR 2020 FEDERAL INFORMATION SECURITY MODERNIZATION ACT 2014 EVALUATION REPORT 23 (2020).

[266] *About the U.S. Dep't of Agriculture*, U.S. DEP'T OF AGRIC., https://www.usda.gov/our-agency/about-usda.

[267] U.S. DEP'T OF AGRIC., PRIVACY IMPACT ASSESSMENT DIRECT LOAN SYSTEM § 3.1 (2009).

[268] *Supplemental Nutrition Assistance Program (SNAP)*, U.S. DEP'T OF AGRIC., https://www.fns.usda.gov/snap/supplemental-nutrition-assistance-program.

[269] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 18-145, HIGH-CONTAINMENT LABORATORIES: COORDINATED ACTIONS NEEDED TO ENHANCE THE SELECT AGENT PROGRAM'S OVERSIGHT OF HAZARDOUS PATHOGENS 3, 9 (2017).

[270] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 18-155, BIODEFENSE: FEDERAL EFFORTS TO DEVELOP BIOLOGICAL THREAT AWARENESS 46 (2017).

[271] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF AGRIC., 50503-0003-12, FISCAL YEAR 2020 FEDERAL INFORMATION SECURITY MODERNIZATION ACT 7 (2020).

[272] *Id.*

[273] *Id.* at 8.

[274] *Id.* at 10.

that are difficult to mitigate effectively.[275] The Inspector General noted USDA's use of unsupported software in FY 2009, 2014, 2015, 2016, 2018, and 2020.[276]

Failure to Remediate Vulnerabilities. According to Department policy, all vulnerabilities rated high, moderate, or low risk should be remediated within 30 days.[277] Under the same policy, critical vulnerabilities must be resolved within 14 days.[278] Despite these requirements, "a significant number of critical network vulnerabilities" were not corrected within 14 days including uninstalled patches and updates.[279] The Inspector General also found "a significant number of high vulnerabilities on selected agencies' public-facing websites that were unknown to the agencies."[280]

> ***The Inspector General also found "a significant number of high vulnerabilities on selected agencies' public-facing websites that were unknown to the agencies."***

Challenges with vulnerability remediation is a common weakness cited by the USDA Inspector General. For example, in FY 2018, 49 percent of critical and high vulnerabilities were outstanding for two-to-five years at one USDA sub-agency.[281] Prolonged remediation timeframes are problematic because "the longer the known vulnerability is exposed on the network, the greater the risk that the vulnerability could be exploited."[282]

Failure to Provide for the Adequate Protection of PII. Auditors determined USDA's outdated policies and procedures "led to decentralized governance of personally identifiable information (PII) throughout the Department."[283] Moreover, practices governing PII "were inconsistently implemented and reflected no overarching policy in place, and no evidence that Departmental policies were communicated and understood by agency stakeholders."[284]

---

[275] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF AGRIC., 50501-0018-12, FISCAL YEAR 2018 FEDERAL INFORMATION SECURITY MODERNIZATION ACT 11 (2018).
[276] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF AGRIC., 50501-15-FM, FISCAL YEAR 2009 FEDERAL INFORMATION SECURITY MANAGEMENT ACT 4 (2009); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF AGRIC., 50501-0006-12, FISCAL YEAR 2014 FEDERAL INFORMATION SECURITY MANAGEMENT ACT 18 (2014); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF AGRIC., 50501-0008-12, FISCAL YEAR 2015 FEDERAL INFORMATION SECURITY MODERNIZATION ACT 16 (2015); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF AGRIC., 50501-0012-12, FISCAL YEAR 2016 FEDERAL INFORMATION SECURITY MODERNIZATION ACT 24 (2016); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF AGRIC., 50501-0018-12, FISCAL YEAR 2018 FEDERAL INFORMATION SECURITY MODERNIZATION ACT 11 (2018); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF AGRIC., 50503-0003-12, FISCAL YEAR 2020 FEDERAL INFORMATION SECURITY MODERNIZATION ACT 10 (2020).
[277] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF AGRIC., 50503-0003-12, FISCAL YEAR 2020 FEDERAL INFORMATION SECURITY MODERNIZATION ACT 10 (2020).
[278] *Id.*
[279] *Id.*
[280] *Id.*
[281] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF AGRIC., 50501-0018-12, FISCAL YEAR 2018 FEDERAL INFORMATION SECURITY MODERNIZATION ACT 10 (2018).
[282] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF AGRIC., 50503-0003-12, FISCAL YEAR 2020 FEDERAL INFORMATION SECURITY MODERNIZATION ACT 10 (2020).
[283] *Id.* at 12.
[284] *Id.*

F. The Department of Health and Human Services

The Department of Health and Human Services' (HHS) mission is "to enhance and protect the health and well-being of all Americans . . . ."[285] HHS seeks to execute that mission "by providing for effective health and human services and by fostering sound, sustained advances in the sciences, underlying medicine, public health, and social services."[286]

HHS has a wealth of sensitive information. For example, the Centers for Medicare and Medicaid Services' houses PII including names, medical information, dates of birth, household income, and employment information.[287] The Centers for Disease Control and Prevention conducts research on deadly diseases and pathogens and operates highly secure research labs called high containment labs, including the highest security labs—biosafety level 4 facilities (BSL-4). CDC uses BSL-4 facilities for research on the most deadly diseases and viruses, such as ebolavirus and smallpox.[288]

HHS was ineffective in each of the five NIST function areas.[289] The Department's overall information security program received a Level 3, "Consistently Implemented" rating.[290] This falls short of the Level 4, "Managed and Measurable" rating necessary for an effective information security program.

Failure to Remediate Vulnerabilities. The Inspector General noted several weaknesses related to HHS's vulnerability management. First, four HHS sub-agencies "did not employ automated mechanisms . . . to detect unauthorized hardware, software, and firmware on its network . . . ."[291] In a similar way, two HHS sub-agencies failed to "centrally manage [their] flaw remediation process and [utilize] automated patch management and software update tools . . . ."[292] Finally, two sub-agencies did not use DHS's EINSTEIN 3 Accelerated capabilities "to detect and proactively block cyber-attacks or prevent potential compromises,"[293] which has been required by Federal law for nearly five years.[294]

---

[285] *About HHS*, U.S. DEP'T OF HEALTH & HUMAN SERVS., https://www hhs.gov/about/index html.
[286] *Id.*
[287] U.S. DEP'T OF HEALTH & HUMAN SERVS., PRIVACY IMPACT ASSESSMENT MARKETPLACE CONSUMER RECORD, (2016); U.S. DEP'T OF HEALTH & HUMAN SERVS., PRIVACY IMPACT ASSESSMENT MEDICARE APPEALS SYSTEM, (2017).
[288] *E.g.*, *High Containment Laboratories at CDC—Fifty Years of Excellence*, CTRS. FOR DISEASE CONTROL & PREVENTION, https://www.cdc.gov/ncezid/dhcpp/hcl-50/high-containment-laboratories html.
[289] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HEALTH & HUMAN SERVS., A-18-20-11200, REVIEW OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES' COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2020 9 (2021).
[290] *Id.*
[291] *Id*. at app. C at 5.
[292] *Id.* at 6.
[293] *Id.* at 16.
[294] Consolidated Appropriations Act § 223(b), Pub. L. No. 114-113, Title II, Subtitle B−Federal Cybersecurity Enhancement Act, 129 Stat. 2963, 2966 (2015), 6 U.S.C. § 1501. *See also supra* Part III. C.

In its review of enterprise-wide implementation of information security and continuous monitoring (ISCM), the HHS Inspector General revealed a concerning gap in HHS's control over cybersecurity at its subordinate operating divisions. Following a finding that HHS operating divisions were not all implementing ISCM,[295] the Inspector General recommended HHS leadership update the Department's ISCM strategy to include a roadmap for ISCM deployment at each HHS division.[296] ISCM is important because it helps both department leadership and HHS operating division leaders see where their cybersecurity gaps are, like unpatched systems and shadow IT.[297] That in turn allows HHS IT officials to fix those issues and secure their network. But HHS disagreed with the recommendation. HHS responded that effectively it lacked the authority to direct information security policy at its subordinate divisions, writing "[d]ue to HHS' federated environment, we cannot force the [operating divisions] to use specific CDM tools or control how much they mature those tools."[298] The Inspector General disagreed, writing "We believe that HHS management is responsible for establishing performance metrics and measures for CDM roll-out and adoption,"[299] a position that appears supported by the goal of the *Federal Information Technology Acquisition Reform Act* to increase the authority of Department CIOs and CISOs across their subordinate agencies.[300]

> ***Two sub-agencies did not use DHS's EINSTEIN 3 Accelerated capabilities "to detect and proactively block cyber-attacks or prevent potential compromises," which has been required by Federal law for nearly five years.***

The Inspector General also identified these weaknesses in FY 2015 and 2016.[301]

Failure to Compile an Accurate and Comprehensive IT Asset Inventory. Like many other federal agencies, HHS struggles to maintain accurate IT asset inventories. The Department's rating in this area fell below the effective level, and one sub-agency "had an Ad Hoc process for using standard data elements to maintain an up-to-date inventory of hardware assets connected to its

[295] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HEALTH & HUMAN SERVS., A-18-20-11200, REVIEW OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES' COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2020 5 (2021).
[296] *Id.* at 6.
[297] *Id.* at 5.
[298] *Id.* at 7, 57.
[299] *Id.* at 7.
[300] National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113-291, Title VIII, Subtitle D—Federal Information Technology Acquisition Reform Act § 831, 128 Stat. 3438 (2014) (commonly known as the Federal Information Technology Acquisition Reform Act).
[301] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HEALTH & HUMAN SERVS., A-18-15-30300, REVIEW OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES' COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2015 17 (2016); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HEALTH & HUMAN SERVS., A-18-16-30350, REVIEW OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES' COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2016 5 (2017).

network."[302] Four sub-agencies also failed to "ensure that the software assets on the network . . . are subject to the monitoring processes" defined under Department policy.[303] The Inspector General has identified this issue in the last three consecutive audits.[304]

Failure to Provide for the Adequate Protection of PII. The Inspector General cited several weaknesses with HHS's protection of PII. This is problematic because HHS maintains significant quantities of PII "including systems that support the Medicare program and its 60 million beneficiaries."[305] As an example, one sub-agency did "not ensure that the security control for protecting PII and other agency sensitive data" were appropriately monitored according to Department policy.[306] Moreover, two sub-agencies "did not measure the effectiveness of [their] data exfiltration and enhanced network defenses by conducting exfiltration exercises."[307] The Department's overall data protection and privacy program is ineffective because HHS components did not "consistently implement[] security controls to protect its PII and other sensitive data."[308] The Inspector General also flagged this issue in FY 2019.[309]

Finally, when evaluating HHS's incident response, the Inspector General also expressed concerns with Department's process for determining whether a cyber incident, such as a hack of HHS's networks, should be defined as a major incident, requiring notification to Congress.[310] The IG warned HHS's process "did not determine whether the incident had or may have had a perceived or actual impact to the American people's public confidence in US Government systems, their civil liberties, or their public health safety."[311] The Inspector General went on to say that in fact HHS "relied upon DHS' . . . determination" and that the decision did not appear to be based on HHS leadership's review and acceptance of that determination, as FISMA requires.[312] HHS disagreed with the finding saying the Department "has never deferred to CISA for any determination."[313]

---

[302] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HEALTH & HUMAN SERVS., INSPECTOR GENERAL SECTION REPORT: 2020 ANNUAL FISMA REPORT app. C at 1 (2021).
[303] *Id.*
[304] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HEALTH & HUMAN SERVS., INSPECTOR GENERAL SECTION REPORT: 2018 ANNUAL FISMA REPORT app. C at 1 (2019); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HEALTH & HUMAN SERVS., INSPECTOR GENERAL SECTION REPORT: 2019 ANNUAL FISMA REPORT app. C at 1 (2020); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HEALTH & HUMAN SERVS., INSPECTOR GENERAL SECTION REPORT: 2020 ANNUAL FISMA REPORT app. C at 1 (2021).
[305] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HEALTH & HUMAN SERVS., A-18-20-11200, REVIEW OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES' COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2020 14 (2021).
[306] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HEALTH & HUMAN SERVICES, INSPECTOR GENERAL SECTION REPORT: 2020 ANNUAL FISMA REPORT, APP. C AT 10 (2021).
[307] *Id.*
[308] *Id.* at 11.
[309] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HEALTH & HUMAN SERVS., INSPECTOR GENERAL SECTION REPORT: 2019 ANNUAL FISMA REPORT app. C at 10 (2020).
[310] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HEALTH & HUMAN SERVS., A-18-20-11200, REVIEW OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES' COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2020 19 (2021).
[311] *Id.*
[312] *Id.*
[313] *Id.* at 61.

G. The Department of Education

The mission of the Department of Education is "to promote student achievement and preparation for global competitiveness by fostering educational excellence and ensuring equal access."[314] In addition, the Department of Education Organization Act directs the Department to "increase the accountability of Federal education programs to the President, the Congress, and the public."[315]

Education's mission requires that it hold substantial quantities of PII and financial information—most notably at the Department's Office of Federal Student Aid (FSA). FSA determines student eligibility for federal student assistance and has sensitive financial information on millions of students and their parents.[316] In FY 2020 alone, FSA processed 17.8 million Free Applications for Federal Student Aid forms and provided $115 billion to 10.8 million students attending 5,600 postsecondary schools.[317]

The Department improved its overall maturity rating, but remains ineffective in all five NIST security functions.[318] According to the Inspector General, until the Department resolves these weaknesses, "it cannot ensure that its overall information security program adequately protects its systems and resources from compromise and loss."[319]

Lack of Valid Authorities to Operate. The Education Inspector General found the Department's system for mobile device management operated without proper authorization for 162 days.[320] This gap in authorization occurred during migration from one software product to another, and was attributed to "a lack of internal communication and information sharing between key stakeholders in OCIO."[321]

Use of Unsupported Systems. Auditors determined the Department relies on systems and applications no longer supported by the vendor.[322] For example, of the 1,341 systems and applications used by the Department, "72 were identified as running with obsolete operating systems."[323] In addition, the Inspector General noted "the Department lacked proper controls to enforce the management of unsupported system components . . . ."[324] Reliance on unsupported technology "could lead to data leakage and exposure of personally identifiable information (PII)

---

[314] *Mission,* U.S. DEP'T OF EDUC., https://www2.ed.gov/about/overview/mission/mission html.
[315] *Id.*
[316] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 18-121, FEDERAL STUDENT AID: BETTER PROGRAM MANAGEMENT AND OVERSIGHT OF POSTSECONDARY SCHOOLS NEEDED TO PROTECT STUDENT INFORMATION 1 (2017).
[317] U.S. DEP'T OF EDUC., FEDERAL STUDENT AID: ANNUAL REPORT FY 2020 XI, 8 (2020).
[318] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF EDUC., ED-OIG/A11U0001, THE U.S. DEPARTMENT OF EDUCATION'S FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 REPORT FOR FISCAL YEAR 2020 2 (2020).
[319] *Id.* at 3.
[320] *Id.* at 62.
[321] *Id.*
[322] *Id.* at 24.
[323] *Id.*
[324] *Id.*

that can compromise the Department's integrity and reputation."[325] The Inspector General made similar findings in FY 2017, 2018, and 2019.[326]

Failure to Remediate Vulnerabilities. The most recent audit found Education failed to consistently apply security patches and updates in a timely fashion.[327] Even more concerning, several systems lacked critical patches increasing their exposure to potential attack.[328] This is a problem at Education because "[t]he Department did not consistently implement and lacked proper controls for enforcing its vulnerability and patch management policies and standards."[329] These weaknesses could expose Education "to a malicious exploit, leakage of data, damage, or unintended exposure of sensitive information."[330] The Inspector General made similar findings in FY 2017, 2018, and 2019.[331]

Failure to Compile an Accurate and Comprehensive IT Asset Inventory. The Inspector General found "the Department was unable to provide sufficient information to validate the completeness of current IT inventory."[332] For instance, Education's systems inventory "did not contain complete system details, such as the system version" and had 652 blank entries.[333] The Department also failed to identify nine of its own websites in its inventory.[334] Finally, Education could not provide sufficient information to substantiate the accuracy of its mobile device inventory.[335] These deficiencies were attributed to the Department's reliance upon "manual and ad-hoc procedures to verify the accuracy of its inventory."[336] Using these ad-hoc procedures "increases the risk a system or device will not be identified or misidentified, and could lead to compromise and exposure of data without the Department knowing that it . . . occurred.[337] The Inspector General last made similar findings in FY 2017 when they discovered 61 active websites not listed on the Department's inventory.[338] If Education's IT staff do not know about a website, they are unable to secure it. Website vulnerabilities are particularly bad because they are publicly accessible to anyone with an

> ***Auditors "successfully transmitted to an external email address a test file containing 200 credit card numbers in a format that should have been blocked according to the Department's policy."***

[325] *Id.*
[326] *Id.*
[327] *Id.* at 23.
[328] *Id.*
[329] *Id.*
[330] *Id.* at 23−24.
[331] *Id.* at 24.
[332] *Id.* at 15.
[333] *Id.*
[334] *Id.*
[335] *Id.*
[336] *Id.* at 16.
[337] *Id.*
[338] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF EDUC., ED-OIG/A11R0001, THE U.S. DEPARTMENT OF EDUCATION'S FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 REPORT FOR FISCAL YEAR 2017 15 (2017).

internet connection, including hackers who may be able to detect those vulnerabilities, and exploit them.

Failure to Provide for the Adequate Protection of PII. Education lacked a consistent oversight process to validate and enforce privacy documents including privacy impact assessments.[339] Without documenting and validating privacy documents "the Department cannot ensure that systems reflect [the] most current privacy risks."[340] These weaknesses limit Education's "ability to protect the privacy of individuals' PII collected, used, maintained, shared, and disposed of by programs and information systems."[341] For example, auditors determined Education's data loss prevention algorithms "were not fully capable of detecting, blocking, or preventing transmission of unencrypted PII and Sensitive PII distributed to . . . external users."[342] During the evaluation, "OIG testers were able to transmit hundreds of sensitive PII/PII [sic] outside of Department controlled networks without being detected."[343] Those same auditors "successfully transmitted to an external email address a test file containing 200 credit card numbers in a format that should have been blocked according to the Department's policy."[344] The Inspector General identified this issue in the last *four* consecutive FISMA audits.[345]

H. The Social Security Administration

The Social Security Administration (SSA) provides benefits to approximately 64 million Americans including retirees, children, widows, and widowers.[346] SSA is charged with protecting some of the most sensitive personal and financial information of American citizens.[347]

SSA houses sensitive financial information on every working and retired American. It houses vast quantities of PII related to its operation of the Title II (Retirement, Survivors, or Disability Insurance) program. This program processes "all post-adjudicative entitlement and payment activities for individuals entitled to Title II benefits."[348] In distributing these benefits, SSA

[339] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF EDUC., ED-OIG/A11U0001, THE U.S. DEPARTMENT OF EDUCATION'S FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 REPORT FOR FISCAL YEAR 2020 37 (2020).
[340] *Id.*
[341] *Id.*
[342] *Id.* at 50.
[343] *Id.* at 53.
[344] *Id.*
[345] OFFICE OF INSPECTOR GEN., U.S. DEP'T OF EDUC., ED-OIG/A11R0001, THE U.S. DEPARTMENT OF EDUCATION'S FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 REPORT FOR FISCAL YEAR 2017 21 (2017); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF EDUC., ED-OIG/A11S0001, THE U.S. DEPARTMENT OF EDUCATION'S FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 REPORT FOR FISCAL YEAR 2018 28 (2018); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF EDUC., ED-OIG/A11T0002, THE U.S. DEPARTMENT OF EDUCATION'S FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 REPORT FOR FISCAL YEAR 2018 29 (2019); OFFICE OF INSPECTOR GEN., U.S. DEP'T OF EDUC., ED-OIG/A11U0001, THE U.S. DEPARTMENT OF EDUCATION'S FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 REPORT FOR FISCAL YEAR 2020 37 (2020).
[346] *About Us*, U.S. SOC. SEC. ADMIN., https://www.ssa.gov/agency/.
[347] *Id.*
[348] U.S. SOC. SEC. ADMIN., 016-00-SSA/DCS-M-001, PRIVACY IMPACT ASSESSMENT TITLE II SYSTEM (2007).

collects names, dates of birth, Social Security numbers, marital status, and earnings data.[349] To qualify for Title II disability insurance, claimants must submit extensive medical records substantiating their impairment.[350]

SSA's information security program was ineffective in four of five NIST security functions.[351] Overall, SSA received a Level 2, "Defined" maturing rating[352]—effectively a D.

As the Inspector General warned in its audit, "SSA houses sensitive information about every individual who has been issued a Social Security number. Inappropriate and unauthorized access to, or theft of, this information can result in significant harm and distress to millions of Americans."[353]

Lack of Valid Authorities to Operate. The Inspector General identified systems in SSA's production environment lacking valid authorities to operate.[354] At the time of the audit, "SSA had not fully implemented its plan to transition to ongoing assessments and monitoring of security controls for ongoing security authorizations."[355] The Inspector General flagged this particular issue in FY 2014, 2015, 2016, and 2017.[356]

Use of Unsupported Systems. The Inspector General found weaknesses in a sensitive legacy information system that processes the PII of millions of Americans.[357] In particular, "privileged user access, permissions, and logged activity were not consistently reviewed" for this system.[358] The Inspector General made a similar finding regarding this system in FY 2018.[359]

Failure to Compile an Accurate and Comprehensive IT Asset Inventory. Auditors determined "SSA did not maintain its inventory of related hardware and software components at a level of granularity necessary for tracking and reporting to management."[360] In addition, although SSA

---

[349] *Id.*
[350] *See Disability Evaluation Under Social Security*, U.S. SOC. SEC. ADMIN., https://www.ssa.gov/disability/professionals/bluebook/index.htm.
[351] OFFICE OF INSPECTOR GEN., U.S. SOC. SEC. ADMIN., A-14-19-50854, THE SOCIAL SECURITY ADMINISTRATION'S INFORMATION SECURITY PROGRAM AND PRACTICES FOR FISCAL YEAR 2020 5 (2020).
[352] *Id.*
[353] *Id.* at 8.
[354] *Id.* at 6.
[355] *Id.* at 9.
[356] OFFICE OF INSPECTOR GEN., U.S. SOC. SEC. ADMIN., A-14-14-24083, THE SOCIAL SECURITY ADMINISTRATION'S COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002 FOR FISCAL YEAR 2014 B-13 (2014); OFFICE OF INSPECTOR GEN., U.S. SOC. SEC. ADMIN., A-14-16-50037, THE SOCIAL SECURITY ADMINISTRATION'S COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2015 B-18, B-19 (2015); OFFICE OF INSPECTOR GEN., U.S. SOC. SEC. ADMIN., A-14-17-50151, THE SOCIAL SECURITY ADMINISTRATION'S COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2016 B-4 (2016); OFFICE OF INSPECTOR GEN., U.S. SOC. SEC. ADMIN., A-14-18-50258, THE SOCIAL SECURITY ADMINISTRATION'S COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2017 7 (2017).
[357] OFFICE OF INSPECTOR GEN., U.S. SOC. SEC. ADMIN., A-14-19-50854, THE SOCIAL SECURITY ADMINISTRATION'S INFORMATION SECURITY PROGRAM AND PRACTICES FOR FISCAL YEAR 2020 8 (2020).
[358] *Id.*
[359] OFFICE OF INSPECTOR GEN., U.S. SOC. SEC. ADMIN., A-14-18-50505, THE SOCIAL SECURITY ADMINISTRATION'S INFORMATION SECURITY PROGRAM AND PRACTICES FOR FISCAL YEAR 2018 8 (2018).
[360] OFFICE OF INSPECTOR GEN., U.S. SOC. SEC. ADMIN., A-14-19-50854, THE SOCIAL SECURITY ADMINISTRATION'S INFORMATION SECURITY PROGRAM AND PRACTICES FOR FISCAL YEAR 2020 7 (2020).

had a policy for maintaining a comprehensive inventory, it "did not include how often the inventory should be updated and how interfaces between systems were maintained."[361] The Inspector General identified similar issues in FY 2016, 2017, and 2018.[362]

Failure to Provide for the Adequate Protection of PII. SSA did not complete and document "procedures for identifying which systems process or store privacy information in SSA's information system inventory."[363] Auditors also found SSA did not sufficiently protect PII or apply appropriate access management controls—this includes the failure to implement several requirements in the *Federal Cybersecurity Enhancement Act of 2015*.[364] The Inspector General found related PII security weaknesses in FY 2016, 2017, and 2018.[365]

SSA houses sensitive financial information on every working and retired American. It houses vast quantities of PII related to its operation of the Title II (Retirement, Survivors, or Disability Insurance) program.

In its response to the most recent Inspector General findings, the Social Security Administration indicated that "FISMA criteria do not provide a holistic view of our program's maturity."[366] As an example, SSA criticized FISMA criterion providing that "any negative control sample in a particular area" reduced their maturity score to two, and that they could only have reached a level four score if there had been zero control failures in the area.[367] They advised that "[t]his binary approach does not provide us with much insight into the relative maturity of our program . . . nor does it do much to help inform our decisions to prioritize and budget our efforts to address issues effectively."[368] SSA suggested a more useful evaluation would be a "framework and approach that assesses maturity

---

[361] *Id.*

[362] OFFICE OF INSPECTOR GEN., U.S. SOC. SEC. ADMIN., A-14-17-50151, THE SOCIAL SECURITY ADMINISTRATION'S COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2016 4, 6 (2016); OFFICE OF INSPECTOR GEN., U.S. SOC. SEC. ADMIN., A-14-18-50258, THE SOCIAL SECURITY ADMINISTRATION'S COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2017 6 (2017); OFFICE OF INSPECTOR GEN., U.S. SOC. SEC. ADMIN., A-14-18-50505, THE SOCIAL SECURITY ADMINISTRATION'S COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2018 6 (2018).

[363] OFFICE OF INSPECTOR GEN., U.S. SOC. SEC. ADMIN., A-14-19-50854, THE SOCIAL SECURITY ADMINISTRATION'S INFORMATION SECURITY PROGRAM AND PRACTICES FOR FISCAL YEAR 2020 8 (2020).

[364] *Id.*; Federal Cybersecurity Enhancement Act of 2015, Pub. L. No. 114-113, Title II, Subtitle B–Federal Cybersecurity Enhancement Act, 129 Stat. 2963 (2015), 6 U.S.C. § 1501. *See also supra* Part III. C.

[365] OFFICE OF INSPECTOR GEN., U.S. SOC. SEC. ADMIN., A-14-17-50151, THE SOCIAL SECURITY ADMINISTRATION'S COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2016 7 (2016); OFFICE OF INSPECTOR GEN., U.S. SOC. SEC. ADMIN., A-14-18-50258, THE SOCIAL SECURITY ADMINISTRATION'S COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2017 8, 9 (2017); OFFICE OF INSPECTOR GEN., U.S. SOC. SEC. ADMIN., A-14-18-50505, THE SOCIAL SECURITY ADMINISTRATION'S COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2018 9, B-18 (2018).

[366] OFFICE OF INSPECTOR GENERAL, U.S. SOC. SEC. ADMIN., A-14-19-50854, THE SOCIAL SECURITY ADMINISTRATION'S COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2020 at 54 (2020).

[367] *Id.* at 54–55.

[368] *Id.*

and clear forward progress . . . ."[369] The Inspector General responded that "testing was performed under generally accepted government auditing standards, which includes the use of the *Financial Audit Manual* sampling methodology to test the design and operating effectiveness of SSA-defined internal controls" as they relate to FISMA metrics.[370]

III. CONCLUSION

Large-scale cyber incidents like SolarWinds and Microsoft Exchange illustrate the considerable threats facing federal agencies. These attacks also make the longstanding vulnerabilities repeatedly documented by Inspector Generals all the more concerning. Unpatched critical vulnerabilities and shadow IT make breaching agencies' networks and stealing sensitive data easier and cheaper, at a time when the Federal Government should be making it harder and more expensive. The Committee will continue to track federal agency implementation of FISMA requirements to ensure agencies fulfill FISMA's primary legislative objective to secure federal networks.

[369] *Id.* at 55.
[370] *Id.* at 12.