CORD

Federal Cybersecurity: America's Data at Risk

Item Type	Senate Bipartisan Staff Report
Download date	2025-02-10 02:16:24
Link to Item	https://hdl.handle.net/20.500.14300/396

United States Senate
PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
Committee on Homeland Security and Governmental Affairs

Rob Portman, Chairman
Tom Carper, Ranking Member

FEDERAL CYBERSECURITY: AMERICA'S DATA AT RISK

STAFF REPORT

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

UNITED STATES SENATE

FEDERAL CYBERSECURITY: AMERICA'S DATA AT RISK

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

Federal government agencies are the frequent target of cybersecurity attacks. From 2006 to 2015, the number of cyber incidents reported by federal agencies increased by more than 1,300 percent. In 2017 alone, federal agencies reported 35,277 cyber incidents. The Government Accountability Office ("GAO") has included cybersecurity on its "high risk" list every year since 1997.

No agency is immune to attack and the list of federal agencies compromised by hackers continues to grow. In the past five years, agencies reporting data breaches include the United States Postal Service, the Internal Revenue Service, and even the White House. One of the largest breaches of government information occurred in 2015 when a hacker ex-filtrated over 22 million security clearance files from the Office of Personnel Management ("OPM"). Those files contained extensive personal and potentially comprising information. We may never know the full impact on our national security of the OPM breach.

The number of data breaches agencies have reported in recent years is not surprising given the current cybersecurity posture of the federal government. A recent report by the Office of Management and Budget ("OMB") made clear that agencies "do not understand and do not have the resources to combat the current threat environment." This is especially concerning given the information agencies must collect and hold. This report documents the extent to which the federal government is the target of cybersecurity attacks, how key federal agencies have failed to address vulnerabilities in their IT infrastructure, and how these failures have left America's sensitive personal information unsafe and vulnerable to theft.

Federal agencies hold sensitive information. The federal government holds extensive amounts of highly personal information on most Americans. For example, the Department of Education collects financial data on students and parents applying for college loans. Disabled Americans prove they are entitled to disability benefits from the Social Security Administration by providing years of health records documenting medical issues. Prospective homeowners provide payroll and savings information to the Department of Housing and Urban Development to qualify for home loans. The Department of Homeland Security maintains travel records on citizens traveling abroad and returning to the United States.

Federal agencies also hold information pertaining to national security and other vital government functions, some of which could be dangerous in the wrong hands. The Department of State holds and vets visa information for foreign nationals applying to come to the United States. The Department of Transportation certifies aircraft through the review of aircraft design, flight test information, and

maintenance and operational suitability. The Department of Agriculture maintains information on hazardous pathogens and toxins that could threaten animals or plants.

Protecting this information from cybersecurity attacks could not be more important.

Congress required OMB and agencies to secure federal networks. In 2002, Congress recognized the importance of protecting information held by the government by passing the Federal Information Security Management Act. That law put OMB in charge of federal cybersecurity, required agencies to provide cybersecurity training for employees, and mandated agencies develop procedures for identifying, reporting, and responding to cyber incidents. Twelve years later, in 2014, Congress updated the law through the Federal Information Security Modernization Act ("FISMA"). The new law reaffirmed OMB's ultimate authority over federal cybersecurity and its responsibility for guiding and overseeing agencies' individual cybersecurity efforts. It also directed the Department of Homeland Security ("DHS") to "administer the implementation of agency [cyber] security policies and practices." This includes activities related to monitoring federal networks and detecting and preventing attacks aimed at federal agencies. DHS also develops directives implementing OMB cybersecurity policies. These directives mandate that federal agencies take certain actions to protect information and systems from emerging cybersecurity threats. In doing so, DHS consults with the National Institute of Science and Technology's ("NIST") to ensure its directives are consistent with NIST's cybersecurity framework. That framework "is a risk-based approach to managing cybersecurity risk" with five core functions essential to an effective approach to cybersecurity:

(1) **Identify** (develop the organizational understanding to manage cybersecurity);
(2) **Protect** (develop and implement the appropriate cybersecurity safeguards);
(3) **Detect** (develop and implement the appropriate activities to identify a cybersecurity event);
(4) **Respond** (develop and implement the appropriate activities to take action in response to the detection of a cybersecurity event); and
(5) **Recover** (develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities impaired due to a cybersecurity event).

Congress also tasked each agency's Inspector General ("IG") to annually audit compliance with basic cybersecurity standards based on the NIST cybersecurity framework. The Subcommittee reviewed the past ten years of audits for DHS and seven other agencies: (1) the Department of State ("State"); (2) the

Department of Transportation ("DOT"); (3) the Department of Housing and Urban Development ("HUD"); (4) the Department of Agriculture ("USDA"); (5) the Department of Health and Human Services ("HHS"); (6) the Department of Education ("Education"); and (7) the Social Security Administration ("SSA"). These seven agencies were cited by OMB as having the lowest ratings with regard to cybersecurity practices based on NIST's cybersecurity framework in fiscal year 2017.

Agencies currently fail to comply with basic cybersecurity standards. During the Subcommittee's review, a number of concerning trends emerged regarding the eight agencies' failure to comply with basic NIST cybersecurity standards. In the most recent audits, the IGs found that seven of the eight agencies reviewed by the Subcommittee failed to properly protect personally identifiable information ("PII"). Five of the eight agencies did not maintain a comprehensive and accurate list of information technology ("IT") assets. Without a list of the agency's IT assets, the agency does not know all of the applications operating on its network. If the agency does not know the application is on its network, it cannot secure the application. Six of the eight agencies failed to install security patches. Vendors issue security patches to secure vulnerabilities. Hackers exploit these vulnerabilities during data breaches. Depending on the vulnerability and abilities of the hacker, the vulnerability may allow access to the agency's network. Multiple agencies, across multiple years, failed to ensure systems had valid authorities to operate. An authority to operate certifies that the system is in proper working order, including an analysis and acceptance of any risk the system may contain. All of the agencies used legacy systems that were costly and difficult to secure. Legacy systems are systems a vendor no longer supports or issues updates to patch cybersecurity vulnerabilities.

The IG audits identified several highly concerning issues at certain agencies. For example, the Education IG found that since 2011, the agency was unable to prevent unauthorized outside devices from easily connecting to the agency's network. In its 2018 audit, the IG found the agency had managed to restrict unauthorized access to 90 seconds, but explained that this was enough time for a malicious actor to "launch an attack or gain intermittent access to internal network resources that could lead to" exposing the agency's data. This is concerning because that agency holds PII on millions of Americans.

Agencies historically failed to comply with cybersecurity standards. The failures cited above are not new. Inspectors General have cited many of these same vulnerabilities for the past decade. The IGs identified several common historical failures at the eight agencies reviewed by the Subcommittee:

Protection of PII. Several agencies failed to properly protect the PII entrusted to their care. These agencies included State, DOT, HUD, Education, and SSA. The HUD IG has noted this issue in *nine* of the last eleven audits.

Comprehensive list of IT assets. The IGs identified a persistent issue with agencies failing to maintain an accurate and comprehensive inventory of its IT assets. In the last decade, IGs identified this as a recurrent problem for State, DOT, HUD, HHS, and SSA.

Remediation of cyber vulnerabilities. Over the past decade, IGs for all eight agencies reviewed by the Subcommittee found each agency failed to timely remediate cyber vulnerabilities and apply security patches. For example, the HUD and State IGs identified the failure to patch security vulnerabilities *seven* of the last ten annual audits. HHS and Education cybersecurity audits highlighted failures to apply security patches *eight* out of ten years. For the last *nine* years, USDA failed to timely apply patches. Both DHS and DOT failed to properly apply security patches for the last *ten* consecutive years.

Authority to operate. The IGs identified multiple agencies that failed to ensure systems had valid authorities to operate. These included DHS, DOT, HUD, USDA, HHS, and Education. For example, HHS systems lacked valid authorities to operate for the last *nine* consecutive audits. Additionally, the DHS IG determined that DHS operated systems without valid authorities in *seven* of the last ten audits. As stated, DHS is the agency in charge of securing the networks of all other government agencies.

Overreliance on legacy systems. The extensive use of legacy systems was also a common issue identified by IGs. All eight agencies examined by the Subcommittee relied on legacy systems. For example, the DHS IG noted the use of unsupported operating systems for at least the last four years, including Windows XP and Windows 2003.

The President's 2019 budget request addressed the risks associated with agencies' reliance on:

> [A]ging legacy systems, [which] pose efficiency, cybersecurity, and mission risk issues, such as ever-rising costs to maintain them and an inability to meet current or expected mission requirements. Legacy systems may also operate with known security vulnerabilities that are either technically difficult or prohibitively expensive to address and thus may hinder agencies' ability to comply with critical cybersecurity statutory and policy requirements.

OMB also recently confirmed the risks legacy systems pose. In May 2018, OMB published the Federal Cybersecurity Risk Determination Report and Action

Plan. OMB explained that the two most substantial issues contributing to agency risk were the "abundance of legacy information technology, which is difficult and expensive to protect, as well as shortages of experienced and capable cybersecurity personnel." That report found that 71 of 96 agencies surveyed (or 74 percent) had cybersecurity programs at risk. Twelve of those 71 agencies had programs at high risk.

Chief Information Officer. In an effort to prioritize agency cybersecurity, Congress established the position of Chief Information Officer ("CIO") in 1996. Since then, Congress has increased the responsibilities of agency CIOs several times. The most recent attempts were included in FISMA and the Federal Information Technology Acquisition Reform Act, which gave CIOs plenary governance over an agency's IT budget and priorities. Despite these authorities, agencies still struggle with empowering the CIO. In August 2018, GAO found that none of the 24 major agencies—including the eight examined by the Subcommittee—properly addressed the role of CIO as Congress directed. These 24 agencies included the eight agencies reviewed by the Subcommittee in this report.

Given the sustained vulnerabilities identified by numerous Inspectors General, the Subcommittee finds that the federal government has not fully achieved its legislative mandate under FISMA and is failing to implement basic cybersecurity standards necessary to protect America's sensitive data.

II. FINDINGS AND RECOMMENDATIONS

Findings of Fact

(1) The Subcommittee reviewed 10 years of Inspectors General reports on compliance with federal information security standards for the Department of Homeland Security and seven other agencies: (1) the Department of State; (2) the Department of Transportation; (3) the Department of Housing and Urban Development; (4) the Department of Agriculture; (5) the Department of Health and Human Services; (6) the Department of Education; and (7) the Social Security Administration.

The Inspectors General reviewed the agencies by assigning ratings based on five security functions established by the National Institutes of Science and Technology ("NIST"): (1) identify; (2) protect; (3) detect; (4) respond; and (5) recover.

For these eight agencies, the Subcommittee found common vulnerabilities described in the latest Inspectors General reports:

- Seven agencies failed to provide for the adequate protection of personally identifiable information;
- Five agencies failed to maintain accurate and comprehensive IT asset inventories;
- Six agencies failed to timely install security patches and other vulnerability remediation actions designed to secure the application; and
- All eight agencies use legacy systems or applications that are no longer supported by the vendor with security updates resulting in cyber vulnerabilities for the system or application.

(2) Several Chief Information Officers ("CIO") for the agencies reviewed by the Subcommittee did not have the authority provided by Congress to make organization-wide decisions concerning information security. This creates confusion about who governs issues of information security and diminishes accountability for the implementation of policies that improve agency cybersecurity.

(3) In May 2018, OMB published a Federal Cybersecurity Risk Determination Report and Action Plan. OMB concluded in the report that the two most significant areas of risk were the abundance of legacy information technology, as well as shortages of experienced and capable cybersecurity

personnel. The Subcommittee determined that all eight agencies reviewed relied on legacy systems.

The Department of Homeland Security

(4) DHS operates the National Cybersecurity Protection System ("NCPS")—commonly known as EINSTEIN—to detect and prevent cyber-attacks. Despite first being introduced in 2013, as of FY 2017 NCPS phase 3 had only been successfully implemented at 65 percent of major agencies.

(5) NCPS's companion program, the Continuous Diagnostics and Mitigation ("CDM") program, provides the capabilities and tools to identify cybersecurity risks on an ongoing basis, prioritize these risks based on potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first. Although DHS has worked to implement several phases, GAO recently concluded that DHS failed to meet the planned implementation dates for each phase.

(6) Since 2014, DHS used its FISMA authority to issue binding operational directives nine times to implement the federal cybersecurity policies, principles, standards, and guidelines set by OMB. These binding operational directives serve as "a compulsory direction to an agency that is for the purposes of safeguarding Federal information and information systems."

(7) In FY 2017, the Department of Homeland Security developed government-wide metrics, aligned with NIST's Cybersecurity Framework, for what constitutes an effective information security program; the agency failed to comply with its own metrics.

(8) **The Department of Homeland Security failed to address cybersecurity weaknesses for at least a decade.** DHS operated systems lacking valid authorities to operate for *seven* consecutive fiscal years. For the last *four* fiscal years, DHS continued to use unsupported systems, such as Windows XP and Windows 2003. For the last *ten* fiscal years, DHS failed to appropriately remediate cyber vulnerabilities by ensuring security patches were properly applied.

The Department of State

(9) In FY 2018, the State Department's information security program ranked among the worst in the federal government. In the Identify and Detect NIST security functions, the State Department received "Ad-hoc" maturity ratings, the lowest possible rating under NIST standards. An Ad-hoc

rating means that the Department has not formalized its cyber policies and procedures and security activities are performed in a reactive manner.

(10) The State Department had reoccurring cybersecurity vulnerabilities, some of which were outstanding for over five years. IG auditors cited State's failure to properly remediate cyber vulnerabilities *seven* times between FY 2008 and 2018. Since FY 2008, the IG noted State's inability to compile an accurate IT asset inventory in *seven* annual FISMA audits. The IG also determined that State failed to adequately protect personally identifiable information *five* times over that same period.

The Department of Transportation

(11) In FY 2018, the Department of Transportation's information security program was ineffective in all five NIST security functions, receiving the second lowest NIST maturity rating in each of the five functions.

(12) The Inspector General identified cybersecurity weaknesses that were outstanding for at least ten years. In *nine* out of the last eleven fiscal years, the IG found that DOT maintained systems lacking valid authorities to operate. For *ten* consecutive years, the IG found DOT failed to remediate vulnerabilities in a timely fashion. In *every* fiscal year since 2008, the IG found DOT failed to compile an accurate IT asset inventory. Finally, since FY 2008 annual FISMA audits documented that DOT failed to adequately protect PII *six* times.

The Department of Housing and Urban Development

(13) In FY 2018, the Department of Housing and Urban Development's information security program was ineffective in all five NIST functions. HUD does not have a mature process for monitoring network and web application data exfiltration. This is problematic because the IG identified several web applications that allow users to generate reports containing PII.

(14) The Department of Housing and Urban Development's annual FISMA audits have continuously highlighted the same cybersecurity weaknesses. The HUD IG highlighted the Department's operation of systems lacking valid authorities to operate in *four* audits since FY 2008. For the last *seven* consecutive years, the Department used unsupported systems and failed to properly apply security patches. Since FY 2008, IG reports cited HUD's failure to compile an accurate IT asset

inventory *eight* times. In *nine* of the last eleven fiscal years, HUD failed to institute policies that adequately protected PII.

The Department of Agriculture

(15) In FY 2018, the Department of Agriculture's cybersecurity program was ineffective in all five NIST functions, with pronounced issues in vulnerability remediation. For example, one USDA sub-agency had 49 percent of critical and high vulnerabilities outstanding for more than two years, and some went unaddressed for over five years.

(16) **The Department of Agriculture had reoccurring cybersecurity issues that have persisted for as long as ten years.** In *every* year since FY 2009, the IG found USDA maintained systems without valid authorities to operate. Over that same timeframe, *five* FISMA audits noted USDA's operation of unsupported systems. Since FY 2008, USDA also failed to properly remediate vulnerabilities *nine* times.

The Department of Health and Human Services

(17) In FY 2018, the Department of Health and Human Services' cybersecurity program was rated ineffective in all five NIST functions. Auditors identified particular issues with HHS's operation of systems lacking valid authorities to operate.

(18) **The Department of Health and Human Services had longstanding cybersecurity weaknesses, including some identified nearly a decade ago.** Auditors found HHS operated systems lacking valid authorities to operate in *nine* consecutive FISMA reviews. In *nine* audits since FY 2008, auditors found HHS used unsupported systems. Over the past eleven fiscal years, HHS failed to properly apply security patches and remediate vulnerabilities *eight* times. Finally, although the issue has been noted *nine* times since FY 2008, HHS still has not compiled an accurate and comprehensive IT asset inventory.

The Department of Education

(19) In FY 2018, the Department of Education's information security program was ineffective according to FISMA standards. Millions of students trust the Department to keep their personal information secure.

The Department of Education had reoccurring cybersecurity weaknesses that impeded the Department's ability to achieve an effective information security program. The IG documented the

agency's operation of systems lacking a valid authority to operate *seven* times since FY 2008. Over that same time, auditors found the Department of Education failed to properly address vulnerabilities and adequately protect PII in *eight* annual FISMA audits.

The Social Security Administration

(20) In FY 2018, the Social Security Administration's information security program was rated ineffective with particular issues related to identity and access management.

The Social Security Administration had persistent cybersecurity issues risking the exposure of the personal information of 60 million Americans who receive Social Security benefits. In *six* of the past eleven fiscal years, FISMA audits determined SSA had deficiencies involving the timely installation of security patches. SSA's lack of a comprehensive IT asset inventory was also identified in *seven* audits during that same time. Most importantly, auditors noted SSA's failure to adequately protect PII *eight* in reports since FY 2008.

Reliance on Vulnerable Legacy Systems

(21) The federal government relies on legacy systems that are costly to maintain and difficult secure. It is unclear what the federal government is spending to maintain legacy systems; certain agencies were unable to tell the Subcommittee the cost of legacy systems. A few examples of legacy systems are below:

- First introduced in the early 1990s, the State Department's Diversity Visa Information System is approximately 29 years old. The application is used by the State Department to track and validate visa application information submitted by foreign nationals.

- HUD's Computer Homes Underwriting Management System ("CHUMS") is approximately 35 years old. CHUMS is so old that lenders are unable to submit loan applications electronically and instead are required to submit them in hard copy through the mail. The application is used by the agency "to initiate and track loan case numbers and associated data."

- First launched in 1998, USDA's Resource Ordering and Status System ("ROSS") is approximately 21 years old. ROSS was supposed to be retired in 2018, but remains in use by the agency. The U.S. Forest Service warns that "the technology used by ROSS is on the verge of

technical obsolescence." This application is used by the Department to deploy resources "including qualified individuals, teams, aircraft, equipment, and supplies to fight wildland fires and respond to all hazard incidents."

- SSA's Title II system that holds retirement and disability information on millions of Americans was first introduced 34 years ago. Some of the Title II subsystems are written in COBOL, which is a programming language first developed in the 1950s and 1960s. As IT professionals who know how to use COBOL leave the workforce, operation costs will continue to rise because of the decrease in people with the necessary background in COBOL.

Recommendations

(1) OMB should require agencies to adopt its risk-based budgeting model addressing blind IT spending. This process links agency IT spending to FISMA metrics to help agencies identify cybersecurity weaknesses that place the security of agency information at risk. Agencies currently use their limited IT funds on capabilities for perceived security weaknesses instead of using those funds on the security risks most likely to be exploited by hostile actors. OMB should report to Congress whether legislation is needed.

(2) Federal agencies should consolidate security processes and capabilities commonly referred to as Security Operations Centers ("SOCs"). This would provide agencies with better visibility across their networks. With this visibility, agencies could better detect cybersecurity incidents and exfiltration attempts.

(3) OMB should ensure that CIOs have the authority to make organization-wide decisions regarding cybersecurity. This authority was provided to CIOs in 2014 with the enactment of FISMA, but the Subcommittee discovered that this is not being implemented as Congress intended. Without this authority, agencies have no senior officer to hold personnel accountable to security standards and implement policies that strengthen the agency's information security program. Congress should consider whether legislation is needed.

(4) OMB should ensure that CIOs are reporting to agency heads on the status of its information security program as mandated by FISMA. Agency heads often exclusively rely upon CIOs and Chief Information Security Officers ("CISO") for matters of information security. This complete delegation detracts from the leadership accountability necessary for agency-wide improvements. To ensure this line of communication, CIOs should submit quarterly reports to agency heads detailing agency performance against FISMA metrics and return on investment for existing cybersecurity capabilities.

(5) Federal agencies should prioritize cyber hiring to fill CIO vacancies and other IT positions critical to agency cybersecurity efforts. To facilitate this prioritization, OMB should determine if additional flexibility is needed across the government for cyber hiring and suggest any legislation necessary to Congress.

(6) **OMB should consider reestablishing CyberStat or regular in-person reviews with agency leadership to focus on cybersecurity issues and generate actionable recommendations to accelerate the fortification of government networks.** OMB should include a summary of the value added by these reviews in its annual FISMA report to Congress.

(7) **In developing shared services for cybersecurity, DHS should consult agency CIOs to ensure that the proposed service will be widely utilized.** When DHS launches a shared service, it should consider piloting the service with a small number of agencies to confirm operability and functionality. As the Quality Service Management Office for cybersecurity, DHS should include a summary of the five-year services implementation plan required by OMB in its annual FISMA report to Congress.

(8) **All federal agencies should include progress reports on cybersecurity audit remediation in their annual budget justification submission to Congress.** Agencies should also include a description of the OMB approved business case in the budget justification for modernized technology or services for which OMB designated a Quality Service Management Office to demonstrate that a separate procurement results in better value.

(9) **Federal agencies should create open cybersecurity recommendation dashboards.** Once created, each agency should submit to Congress every six months metrics on audit recommendation closure rates and accomplishments. Each agency head should also be briefed and approve the agency's plan for addressing open cyber recommendations.

III. BACKGROUND

The importance of cybersecurity protocols has never been greater as millions of Americans cope with the exposure of personal information. The number of cybersecurity incidents at federal agencies increased in 2017 reaffirming the significance of sufficient cybersecurity protections.[1] In light of the uptick in cyber-attacks, federal agencies must implement the strategies and practices necessary to protect themselves from hackers seeking the data they collect and store. Despite congressional mandates, federal agencies repeatedly fail to meet basic cybersecurity standards necessary to protect the sensitive information entrusted to them.[2]

A. Increase in Cybersecurity Incidents

Federal agencies increasingly rely on electronic data storage to maintain records.[3] As a result, the security protocols designed to protect this sensitive information are an integral part of sustaining public confidence in the federal government.[4] Without appropriate safeguards, hackers can steal and exploit sensitive information—including personally identifiable information ("PII") like taxpayer records, medical records, and Social Security numbers.[5]

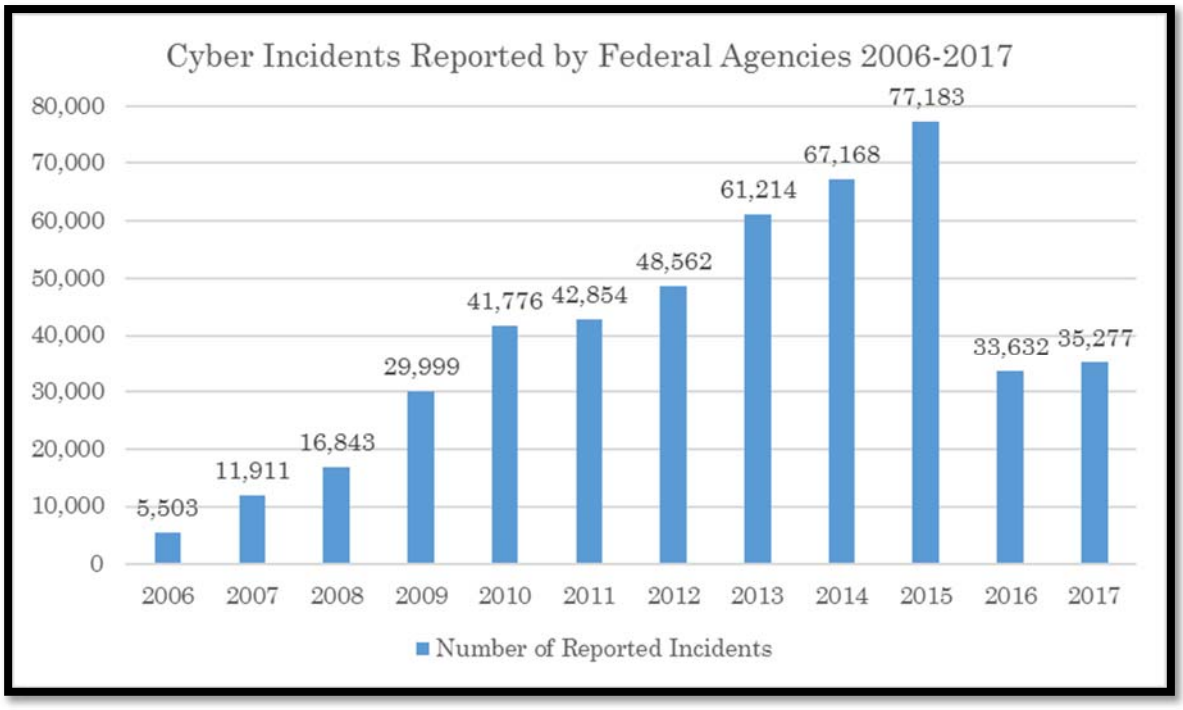
Protecting this data continues to challenge federal agencies. The complexity, technological diversity, and geographical decentralization of government networks present unique challenges for federal cybersecurity experts.[6] These complications make it harder for IT specialists to identify, manage, and protect the numerous operating systems under their purview.[7] Federal agencies are especially prone to cyber-attacks because of frequent interconnection with other internal and external networks "including the Internet, thereby increasing the number of avenues of

---

[1] OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 ANNUAL REPORT TO CONGRESS, 1 (2017).
[2] According to the Government Accountability Office's ("GAO") most recent bi-annual report on the state of federal government information security programming, the vast majority of the 24 agencies covered by the Chief Financial Officers Act ("CFO Act") failed to adequately "protect information system boundaries." U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 17-549, FEDERAL INFORMATION SECURITY: WEAKNESSES CONTINUE TO INDICATE NEED FOR EFFECTIVE IMPLEMENTATION OF POLICIES AND PRACTICES, 17 (SEPT. 2017).
[3] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 16-885T, FEDERAL INFORMATION SECURITY: ACTIONS NEEDED TO ADDRESS CHALLENGES, 1 (SEPT. 19, 2016).
[4] *Id.*
[5] *Id.* at 1–2.
[6] *Id.* at 2.
[7] *Id.*

attack and expanding their attack surface."[8] Such interconnectedness provides hostile actors with various options to exploit system vulnerabilities.[9]

From 2006 to 2015, the number of cyber incidents recorded at federal agencies increased by more than 1,300 percent from 5,503 to 77,183.[10] The chart below details annual cyber incidents reported by federal agencies.



[11]

In 2016, the total number of cyber incidents reported by federal agencies decreased by 56 percent to 33,632.[12] According to a DHS official, this decrease is primarily attributable to revised incident reporting requirements "that no longer require agencies to report non-cyber incidents or attempted scans or probes of agency networks."[13] In 2017, there was roughly a 5 percent increase in the number of cyber incidents reported by government agencies.[14]

---

[8] *Id.*
[9] *Id.*
[10] Joe Davidson, *Federal cyber incidents jump 1,300% in 10 years*, WASH. POST, Sept. 22, 2016.
[11] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 17-440T, CYBERSECURITY: ACTIONS NEEDED TO STRENGTHEN U.S. CAPABILITIES, 4 (FEB. 14, 2017); 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, 6 (DEC. 18, 2018).
[12] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 17-440T, CYBERSECURITY: ACTIONS NEEDED TO STRENGTHEN U.S. CAPABILITIES, 4 (FEB. 14, 2017).
[13] *Id.*
[14] 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, 6 (DEC. 18, 2018).

B. Reliance on Legacy Information Technology

With respect to IT spending, the federal government routinely relies on legacy systems.[15] A legacy system refers to "an outdated or obsolete system of information technology."[16]

In 2018, OMB concluded that one of the most significant areas of federal government cybersecurity risk was "the abundance of legacy information technology, which is difficult and expensive to protect."[17] Increasingly, these systems rely on "outdated languages and old parts."[18] The risk posed by legacy systems was acknowledged in President Trump's May 2017 executive order that stated "the executive branch has for too long accepted antiquated and difficult-to-defend IT."[19]

Due to the outdated languages upon which these systems rely, the cost to maintain legacy systems will continue to increase.[20] This is largely a result of the premium that agencies have to pay for "staff or contractors with knowledge to maintain outdated systems."[21] To address the risk posed by overreliance on legacy IT, the federal government must plan "so that maintenance, improvements, and modernization occur in a coordinated way and with appropriate regularity."[22]

C. The Federal Information Security Management Act of 2002

Prior to the Federal Information Security Management Act's enactment, and as early as 1996, GAO identified the risks associated with the federal government's increased reliance upon information systems. In 1996, GAO noted that "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 government's ability to protect confidential data on individuals."[23] GAO also added that although the information held by federal

---

[15] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 16-696T, INFORMATION TECHNOLOGY: FEDERAL AGENCIES NEED TO ADDRESS AGING LEGACY SYSTEMS, 6 (MAY 25, 2016).
[16] Pub. L. No. 115-91, National Defense Authorization Act for Fiscal Year 2018, Title X, Subtitle G, § 1076(8).
[17] OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, FEDERAL CYBERSECURITY RISK DETERMINATION REPORT AND ACTION PLAN, 2 (2018).
[18] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 16-468, INFORMATION TECHNOLOGY: FEDERAL AGENCIES NEED TO ADDRESS AGING LEGACY SYSTEMS, 26 (MAY 2016).
[19] Exec. Order No. 13800 (2017).
[20] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 16-468, INFORMATION TECHNOLOGY: FEDERAL AGENCIES NEED TO ADDRESS AGING LEGACY SYSTEMS, 28 (MAY 2016).
[21] *Id.*
[22] Exec. Order No. 13800 (2017).
[23] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO/AIMD 96-110, INFORMATION SECURITY: OPPORTUNITIES FOR IMPROVED OMB OVERSIGHT OF AGENCY PRACTICES, 2 (SEPT. 1996).

agencies is often unclassified, it is "extremely sensitive, and many automated operations would be attractive targets for individuals."[24]

Congress first codified permanent cybersecurity expectations for federal agencies in the Federal Information Security Management Act of 2002. This law authorized the expiring information security measures originally contained in the Government Information Security Reform Act ("GISRA").[25] GISRA was enacted as part of the National Defense Authorization Act for Fiscal Year 2001.[26]

As enacted in 2001, GISRA mandated that program managers and Chief Information Officers ("CIO") develop a "risk-based security management program covering all operations and assets of the agency."[27] That legislation also required that each agency conduct an annual independent evaluation of its information security program.[28] The goal was to provide both Congress and OMB with the opportunity to oversee the effectiveness of agency efforts pertaining to information security.[29] In particular, this risk-based security management program had to include:

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

(2) Training for information security employees.

(3) The development of procedures for identifying, reporting, and responding to cyber incidents.[30]

In addition to the aforementioned provisions of GISRA, the Federal Information Security Management Act required the Director of OMB to "establish and operate a central Federal information security incident center" while also promulgating "standards and guidelines pertaining to Federal information systems."[31] The law contained provisions that established for the first time minimum mandatory management controls government-wide instead of providing each agency with the discretion to implement its own system controls.[32]

Even after Congress passed the Federal Information Security Management Act, federal agency information security problems persisted. For example, GAO

---

[24] *Id.*
[25] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 02-677T, INFORMATION SECURITY: COMMENTS ON THE PROPOSED FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002, 2 (MAY 2, 2002).
[26] *Id.* at 1.
[27] *Id.* at 7.
[28] *Id.* at 8.
[29] *Id.*
[30] *Id.* at 6.
[31] CONG. RESEARCH SERV., SUMMARY: THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT (MAR. 5, 2002).
[32] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 02-677T, INFORMATION SECURITY: COMMENTS ON THE PROPOSED FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002, 10 (MAY 2, 2002).

determined that in FY 2012, 23 out of 24 of the major federal agencies maintained deficiencies in controls that prevented them from curtailing or identifying unauthorized access to computer resources.[33] 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."[34]

These findings, among other concerns, prompted Congress to reevaluate the 2002 law.[35] One specific issue GAO identified was that information security roles were unclear throughout the federal government.[36] For example, although the Federal Information Security Management Act granted OMB the lead statutory authority over federal cybersecurity, OMB delegated much of that authority to DHS.[37] This created confusion as to which agency was in charge.[38] Congress also sought to update the 2002 law because of the increase in hacker targeting of vulnerable government IT systems.[39] Lastly, Congress recognized the importance of a new approach to federal cybersecurity because dated and paperwork intensive cybersecurity requirements were preventing agencies from implementing modern security practices that would allow them to better address emerging threats.[40] Following the identification of these weaknesses, the Federal Information Security Modernization Act was enacted on December 18, 2014.[41]

D. The Federal Information Security Modernization Act of 2014

The Federal Information Security Modernization Act ("FISMA") reaffirmed OMB's responsibility to develop and oversee "the implementation of policies, principles, standards, and guidelines on information security."[42] FISMA also tasked OMB with "overseeing agency compliance with the requirements" in the legislation.[43] Unlike its predecessor, FISMA required DHS to "administer the implementation of agency information security policies and practices for information systems."[44]

---

[33] 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 (SEPT. 2013).
[34] *Id.* at 14.
[35] Briefing with the U.S. Gov't Accountability Office (Sept. 19, 2018).
[36] *Id.*
[37] S. Rep. No. 113-256, at 3–5 (2014).
[38] *Id.*
[39] *Id.* at 5.
[40] *Id.* at 6–7.
[41] CONG. RESEARCH SERV., SUMMARY: THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT (DEC. 18, 2014).
[42] Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 44 U.S.C. § 3553(a)(1).
[43] *Id.* at § 3553(a)(5).
[44] *Id.* at § 3553(b).

Under FISMA, Congress required DHS to develop and oversee "the implementation of binding operational directives to agencies to implement the policies, principles, standards, and guidelines" set by OMB.[45] 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."[46] OMB retains the power to revise or repeal these directives if it determines that they are "not in accordance with the policies, principles, standards, and guidelines" developed by OMB.[47] DHS has used this authority nine times to, for example, direct the removal of Kaspersky-branded software deemed a security risk and address vulnerabilities on internet-facing IT systems that leave agencies susceptible to cyber-attack.[48] To promote information security audit uniformity across the federal government, FISMA instructed DHS to consult with NIST to "ensure that binding operational directives" do not conflict with the information security standards set forth by NIST.[49] 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.

To facilitate and streamline the implementation of OMB cybersecurity policies, FISMA required DHS to "[convene] meetings with senior agency officials."[50] The purpose of these meetings was to help DHS determine whether it should provide "operational and technical assistance" to an agency to improve information security.[51] 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."[52] Specifically, these reports must include a summary of major cyber incidents from that year and a summary of the information security program evaluation.[53] In addition, OMB must assess agency compliance with data breach notification procedures established by the Director of OMB.[54]

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 violations of the information security program.[55] Each agency is required to "document, and implement an agency-wide information security

---

[45] *Id.* at § 3553(b)(2).
[46] *Id.* at § 3552(b)(1).
[47] *Id.* at § 3553(b)(2).
[48] *Cybersecurity Directives*, DEP'T OF HOMELAND SECURITY, https://cyber.dhs.gov/directives/.
[49] Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 44 U.S.C. § 3553(f)(2)(A)–(B).
[50] *Id.* at § 3553(b)(4).
[51] *Id.* at § 3553(b)(6).
[52] *Id.* at § 3553(c).
[53] *Id.*
[54] *Id.*
[55] *Id.* at § 3554(a)(1)(A)–(C).

program" and conduct periodic assessments of said program to ensure continued efficiency and cost effectiveness.[56] Moreover, like its predecessor, FISMA required that each agency perform an independent evaluation of its information security program.[57] This evaluation requires each agency to test and assess the "effectiveness of information security policies, procedures, and practices" at the agency.[58]

Finally, FISMA 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.[59] 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."[60] In the event that a major incident occurs, agencies must report that incident no "later than 7 days after the date on which there is a reasonable basis to conclude that [a] major incident has occurred."[61]

1. NIST's Cybersecurity Framework

On December 18, 2014, Congress passed the Cybersecurity Enhancement Act, 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."[62] The Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act defines "critical infrastructure" as "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."[63] These updates addressed the U.S. government's increased reliance upon technology, and the corresponding expansion of potential cyber vulnerabilities.[64]

Pursuant to its legislative mandate under the Cybersecurity Enhancement Act, NIST released Version 1.1 of its *Framework for Improving Critical*

---

[56] *Id.* at § 3554(b)−(b)(1).
[57] *Id.* at § 3555(a).
[58] *Id.* at § 3555(a)(2)(B).
[59] *Id.* at § 3553(b)(6)(A), § 3554(b)(7)(C)(iii)(III).
[60] OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, M-18-02, FISCAL YEAR 2017-2018 GUIDANCE ON FEDERAL INFORMATION SECURITY AND PRIVACY MANAGEMENT REQUIREMENTS, 5 (2017).
[61] Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 44 U.S.C. § 3554(b)(7)(C)(iii)(III)(aa).
[62] Cybersecurity Enhancement Act of 2014, Pub. L. No. 113-274, 15 U.S.C. § 272(c)(15).
[63] The USA PATRIOT Act of 2001, Pub. L. No. 107-56, 42 U.S.C. § 5195c(e).
[64] *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*, NAT. INST. OF STANDARDS & TECHNOLOGY, 1 (Apr. 16, 2018).

Infrastructure Cybersecurity on April 16, 2018.[65] Composed of three parts, the Framework "is a risk-based approach to managing cybersecurity risk."[66] 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."[67] The Framework Core is composed of five functions—Identify, Protect, Detect, Respond, and Recover.[68] Collectively, these functions "provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk."[69]

With the Framework, NIST sought to improve organizational risk management. For this purpose, risk management is defined as "the ongoing process of identifying, assessing, and responding to risk."[70] Specifically, the Framework uses risk management processes "to enable organizations to inform and prioritize decisions regarding cybersecurity."[71] Moreover, it encourages frequent risk assessments "to help organizations select target states for cybersecurity activities that reflect desired outcomes."[72]

2. Executive Order 13800

On May 11, 2017, President Trump signed Executive Order ("EO") 13800 addressing cybersecurity risks.[73] The executive order requires that agencies take certain actions to enhance the nation's capabilities against cybersecurity threats.[74] EO 13800 acknowledges that "the executive branch has for too long accepted antiquated and difficult-to-defend IT."[75] EO 13800 also highlighted that "known but unmitigated vulnerabilities are among the highest cybersecurity risks faced by executive departments and agencies."[76] Examples of those vulnerabilities include "using operating systems or hardware beyond the vendor's support lifecycle, declining to implement a vendor's security patch, or failing to execute security-specific configuration guidance."[77]

---

[65] 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).
[66] *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*, NAT. INST. OF STANDARDS & TECHNOLOGY, 3 (Apr. 16, 2018).
[67] *Id.*
[68] *Id.*
[69] *Id.*
[70] *Id.* at 4.
[71] *Id.*
[72] *Id.*
[73] Exec. Order No. 13800 (2017).
[74] *Id.*
[75] *Id.*
[76] *Id.*
[77] *Id.*

Within the FISMA context, EO 13800 instructs all agencies to use NIST's Cybersecurity Framework in conducting their annual information security program reviews.[78] The EO also makes clear that agency heads will be "held accountable by the President for ensuring that cybersecurity risk management processes are aligned with strategic, operational, and budgetary planning processes, in accordance" with FISMA.[79]

3. OMB and DHS Guidance to Agencies for FISMA Compliance

FISMA 2014 required OMB and DHS to develop and administer guidelines applicable to all federal agencies for the purpose of 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 October 16, 2017, OMB issued Memorandum M-18-02, *Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements*.[80] This memorandum provided reporting guidance and deadlines for federal agencies' annual FISMA obligations.[81] These reporting deadlines require that all civilian agencies submit annual FISMA reports to OMB and DHS by October 31 each year.[82] Agency reports are then due to Congress and GAO by March 1.[83]

In addition to the annual report, Memorandum M-18-02 required each agency head submit a letter to the OMB Director and the Secretary of Homeland Security.[84] This letter must include: (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.[85]

FISMA also directed OMB to define the term "major incident" for agency reporting to Congress.[86] OMB subsequently 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."[87] Memorandum M-

---

[78] *Id.*
[79] *Id.*
[80] OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, M-18-02, FISCAL YEAR 2017-2018 GUIDANCE ON FEDERAL INFORMATION SECURITY AND PRIVACY MANAGEMENT REQUIREMENTS, 1 (2017).
[81] *Id.*
[82] *Id.* at 2.
[83] *Id.* at 4.
[84] *Id.* at 2–3.
[85] *Id.* at 3.
[86] Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 44 U.S.C. § 3558(b).
[87] OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, M-18-02, FISCAL YEAR 2017-2018 GUIDANCE ON FEDERAL INFORMATION SECURITY AND PRIVACY MANAGEMENT REQUIREMENTS, 5 (2017).

18-02 further provides that a breach "constitutes a major incident when it involves personally identifiable information (PII) that, if exfiltrated, modified, deleted, or otherwise compromised" would be damaging to the interests of the United States.[88] OMB guidance also reiterates FISMA's requirement that in the event of a major incident an agency must notify Congress within seven days.[89]

To supplement OMB's FISMA guidance, DHS produces general FISMA metrics each fiscal year. This document assists each agency IG in the annual information security evaluation required by FIMSA. In particular, these metrics "provide reporting requirements across key areas to be addressed in the independent evaluations."[90] 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 and Authorization; Comprehensive Risk Management)
2. **Protect** (Remove Access Protection; Credentialing and Authorization; Network Protection)
3. **Detect** (Anti-Phishing Capabilities; Malware Defense Capabilities; Exfiltration and Other Capabilities)
4. **Respond** (Planning and Processes; Evaluation and Improvement)
5. **Recover** (Planning and Testing; Personal Impact Process; Back-Up Capacity)[91]

Using these metrics, IGs must rate their agencies on each of the five functions contained in NIST's Cybersecurity Framework.[92] These ratings aim to "capture the extent that agencies institutionalize" the requirements set forth in FISMA.[93] The table below summarizes the five possible maturity ratings and their corresponding descriptions:

[88] *Id.* at 5–6.
[89] *Id.* at 6.
[90] U.S. Dep't of Homeland Security, Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics, 4 (Apr. 11, 2018).
[91] OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014: ANNUAL REPORT TO CONGRESS, 25 (2017).
[92] U.S. Dep't of Homeland Security, Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics, 4 (Apr. 11, 2018).
[93] *Id.* at 5.

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.

[94]

For the purposes of this maturity model, if an agency has achieved a Level 4, "Managed and Measurable" rating, it is considered to have achieved an effective security level.[95] When assessing the overall effectiveness of the agency's information security program, DHS guidance encourages IGs to apply a simple majority rule.[96] 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 to be effective.[97]

[94] OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014: ANNUAL REPORT TO CONGRESS, 26 (2017).
[95] U.S. Dep't of Homeland Security, Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics, 5 (Apr. 11, 2018).
[96] *Id.* at 6.
[97] *Id.*

4. Oversight of Agency Compliance with FISMA

To ensure agency accountability, Congress imposed deadlines and oversight requirements in FISMA, including the requirement that agency IGs evaluate their agency's information security program.[98] This requirement was a holdover from the 2002 law.[99] This evaluation must include both testing and an assessment of "the effectiveness of the information security policies, procedures, and practices of the agency."[100] Congress also instructed GAO to provide periodic reports detailing the adequacy of agency information security programs and the steps agencies have taken toward implementing FISMA requirements.[101] Since the Federal Information Security Management Act's passage in 2002 and continuing with FISMA in 2014, each IG has issued an annual report documenting agency compliance and implementation efforts.

FISMA also authorized GAO to provide technical assistance to agency heads or agency IGs.[102] In this role, GAO assists agency officials in carrying out FISMA mandates "by testing information security controls and procedures."[103]

E. Additional Legislation and Executive Action to Promote Improved Federal Government Cybersecurity

Since FISMA's enactment in 2014, Congress has passed additional legislation to address federal government cybersecurity vulnerabilities. Two of these laws are the Federal Information Technology Acquisition Reform Act ("FITARA"), which passed days after FISMA in 2014, and the Modernizing Government Technology Act ("MGT") which passed in December 2017.[104]

1. The Federal Information Technology Acquisition Reform Act

In FY 2018, the President's budget requested $96 billion in total IT funding—"the largest amount ever."[105] Despite this funding request, federal IT investments "often result in failed projects that incur cost overruns and schedule slippages,

---

[98] Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 44 U.S.C. § 3558(a).
[99] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 02-677T, INFORMATION SECURITY: COMMENTS ON THE PROPOSED FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002, 6 (MAY 2, 2002).
[100] Federal Information Security Modernization Act of 2014, at § 3555(a)(2)(A)–(B).
[101] *Id.* at § 3555(h)(1)–(2).
[102] *Id.* at § 3555(i).
[103] *Id.*
[104] PATRICIA MOLONEY FIGLIOLA, CONG. RESEARCH SERV., R44462, THE FEDERAL INFORMATION TECHNOLOGY ACQUISITION REFORM ACT (FITARA): FREQUENTLY ASKED QUESTIONS 1 (2016); U.S. Off. Mgmt. & Budget, Exec. Office of the President, M-18-12, Implementation of the Modernizing Government Technology Act, 1 (Feb. 27, 2018).
[105] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 18-234T, INFORMATION TECHNOLOGY: FURTHER IMPLEMENTATION OF FITARA RELATED RECOMMENDATIONS IS NEEDED TO BETTER MANAGE ACQUISITIONS AND OPERATIONS, 2 (NOV. 15, 2017).

while contributing little to the desired mission-related outcomes."[106] To address this issue, Congress passed FITARA "to improve agencies' acquisitions of IT and enable Congress to monitor agencies' progress and hold them accountable for reducing duplication and achieving cost savings."[107]

FITARA outlines seven main areas addressing "how federal agencies purchase and manage their IT assets."[108] These seven areas include: (1) enhancing the authority of agency CIOs; (2) improving transparency and risk management of IT investments; (3) setting forth a process for agency IT portfolio review; (4) refocusing the Federal Data Center Consolidation Initiative from only consolidation to optimization; (5) expanding the training and use of "IT Cadres," as initially outlined in the "25 Point Implementation Plan to Reform Federal Information Management Technology"; (6) maximizing the benefits of the Federal Strategic Sourcing Initiative (FSSI); and (7) creating a government-wide software purchasing program, in conjunction with the General Services Administration.[109] GAO reports that agencies have made some progress with the implementation of these requirements but that agencies could still realize billions in cost savings if they improve "data center consolidation, [increase] transparency via OMB's IT Dashboard, [implement] incremental development, and [manage] software licenses."[110]

2. The Modernizing Government Technology Act

By passing the MGT Act, Congress sought to "allow agencies to invest in modern technology solutions to improve service delivery to the public, secure sensitive systems and data, and save taxpayer dollars."[111] Two main provisions of the law address IT modernization needs of federal agencies.[112]

First, the MGT Act establishes a Technology Modernization Fund ("TMF") and a Technology Modernization Board ("the Board").[113] Under this new funding model, agencies submit proposals to the Board which reviews them on the basis of "financial, technical, and operational criteria."[114] If an agency receives approval

---

[106] *Id.*
[107] *Id.* at 4.
[108] PATRICIA MOLONEY FIGLIOLA, CONG. RESEARCH SERV., R44462, THE FEDERAL INFORMATION TECHNOLOGY ACQUISITION REFORM ACT (FITARA): FREQUENTLY ASKED QUESTIONS 1 (2016).
[109] *Id.*
[110] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 18-234T, INFORMATION TECHNOLOGY: FURTHER IMPLEMENTATION OF FITARA RELATED RECOMMENDATIONS IS NEEDED TO BETTER MANAGE ACQUISITIONS AND OPERATIONS, 12 (NOV. 15, 2017).
[111] OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, M-18-12, IMPLEMENTATION OF THE MODERNIZING GOVERNMENT TECHNOLOGY ACT, 1 (2018).
[112] *Id.*
[113] *Id.*
[114] *Id.* at 2.

from the Board for TMF funds, the agency receives the money "in an incremental manner, tied to specific project milestones and objectives, and will be regularly monitored by the Board for success."[115] Finally, agencies are required to pay back any TMF funds granted to them in accordance with a written agreement with the Board.[116]

Second, the MGT Act authorized all CFO Act agencies to create Working Capital Funds ("WCFs").[117] Under the law, agencies can only use WCFs for a number of defined purposes.[118] These purposes include: (1) "to improve, retire, or replace existing information technology systems;" (2) "to transition legacy information technology systems to commercial cloud computing;" (3) "to assist and support covered agency efforts to provide adequate, risk-based, and cost-effective information technology capabilities;" (4) "to reimburse funds transferred to the agency from the TMF;" and (5) "for a program, project, or activity or to increase funds for any program, project, or activity that has not been denied or restricted by Congress."[119]

3. Executive Order on America's Cybersecurity Workforce

On May 2, 2019, President Trump issued an Executive Order addressing America's cybersecurity workforce. The order reiterates EO 13800's contention that a "superior cybersecurity workforce will promote American prosperity and preserve peace."[120] In addition, it further emphasizes the importance of cybersecurity professionals as "guardians of our national and economic security."[121]

The order itself required that DHS, in consultation with OMB and OPM, establish "a cybersecurity rotational assignment program, which will serve as a mechanism for knowledge transfer and a development program for cybersecurity practitioners."[122] It also called on the federal government to better facilitate the movement of cybersecurity professionals between the public and private sectors in order to maximize "the contributions made by their diverse skills, experience, and talents to our Nation."[123] In a similar way, the order called on the federal government to also support the continued development of cybersecurity skills and

---

[115] *Id.*
[116] *Id.*
[117] *Id.* at 1.
[118] *Id.* at 4.
[119] *Id.*
[120] Exec. Order on America's Cybersecurity Workforce (May 2, 2019), https://www.whitehouse.gov/presidential-actions/executive-order-americas-cybersecurity-workforce/.
[121] *Id.*
[122] *Id.*
[123] *Id.*

expertise so that "America can maintain its competitive edge in cybersecurity."[124] To cultivate improved cybersecurity skills, the order recommended that the federal government improve access to training opportunities to reduce the Nation's shortage of cybersecurity talent.[125] Finally, the order instructed DHS, DOD, and OMB to establish an annual cybersecurity competition to "identify, challenge, and reward, the United States Government's best cybersecurity practitioners and teams across offensive and defensive cybersecurity disciplines."[126]

F. DHS Efforts to Improve Federal Cybersecurity Posture

On December 18, 2015, Congress passed the Federal Cybersecurity Enhancement Act as part of that year's Consolidated Appropriations Act.[127] The Federal Cybersecurity Enhancement Act "sets forth authority for enhancing federal intrusion prevention and detection capabilities among federal entities."[128]

In particular, this law required that DHS "deploy, operate, and maintain capabilities to prevent and detect cybersecurity risks in network traffic traveling to or from an agency's information system."[129] Moreover, the bill mandated DHS make those capabilities available to all federal agencies.[130] DHS's National Cybersecurity Protection System ("NCPS") and its Continuous Diagnostics and Mitigation ("CDM") program reflect the Department's efforts to improve the cybersecurity posture of the federal government.[131]

1. National Cybersecurity Protection System

DHS describes NCPS as "an integrated system-of-systems that delivers a range of capabilities, including intrusion prevention, analytics, intrusion prevention, and information sharing."[132] Composed of three phases, NCPS, often referred to as "Einstein," is designed to "provide a technological foundation that enables [DHS] to secure and defend the federal civilian government's information technology infrastructure."[133]

The table below lists and summarizes each phase of NCPS:

---

[124] *Id.*
[125] *Id.*
[126] *Id.*
[127] Consolidated Appropriations Act, Pub. L. No. 114-113, 6 U.S.C. § 1501.
[128] 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, 9 (DEC. 18, 2018).
[129] *Id.*
[130] *Id.*
[131] *Id.* at 13.
[132] *National Cybersecurity Protection System (NCPS)*, U.S. Dep't of Homeland Security, https://www.dhs.gov/national-cybersecurity-protection-system-ncps.
[133] *Id.*

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.

134

As shown above, NCPS is now in phase three of its deployment.[135] NCPS's capabilities are "operationally known as the EINSTEIN set of capabilities."[136] Despite being deployed in 2013, as of FY 2017 Einstein 3 had only been successfully implemented at 65 percent of the CFO Act agencies.[137]

In January 2016, GAO issued a report outlining several shortcomings. For example, of the five software applications reviewed by GAO, NCPS intrusion detection signatures "provided some degree of coverage" for roughly 29 of 489 vulnerabilities identified—roughly a six percent success rate.[138] This is problematic because signatures are a crucial intrusion prevention tool, which allow for the detection of "malicious traffic by comparing current traffic to known patterns of malicious behavior."[139]

In that same report, GAO determined that NCPS relied exclusively on signature-based methodologies for intrusion prevention. This detracts from the overall effectiveness of the program because "NCPS is unable to detect intrusions

---

[134] 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 (DEC. 18, 2018).

[135] *Id.*

[136] *National Cybersecurity Protection System (NCPS)*, U.S. Dep't of Homeland Security, https://www.dhs.gov/cisa/national-cybersecurity-protection-system-ncps.

[137] OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014, ANNUAL REPORT TO CONGRESS FISCAL YEAR 2017, 7 (2018).

[138] 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, 22 (JAN. 2016).

[139] *Id.* at 17.

for which it does not have a valid or active signature."[140] Therefore, NCPS did not have the capability to detect any unknown forms of malicious traffic.

In 2018, GAO followed up on the issues it discovered in 2016 and determined that DHS made improvements to NCPS.[141] During this review, DHS told GAO that it was now "operationalizing functionality intended to identify malicious traffic activity in the network traffic otherwise missed by signature-based methods."[142] DHS also improved the tool it uses to track signatures "to include a mechanism to clearly link signatures to publicly available, open-source information."[143]

Despite these improvements, GAO identified NCPS shortcomings, including NCPS's inability "to effectively detect intrusions across multiple types of traffic."[144] In addition, DHS had not instituted metrics for NCPS that provide the Department with "information about how well the system is enhancing government information security."[145] In the absence of these metrics, DHS will be unable to determine the precise value provided by NCPS.[146]

NCPS comes with a significant cost. As of 2016, the projected cost of NCPS through FY 2018 was roughly $5.7 billion.[147] For FY 2018 alone, Congress appropriated $402 million for NCPS.[148]

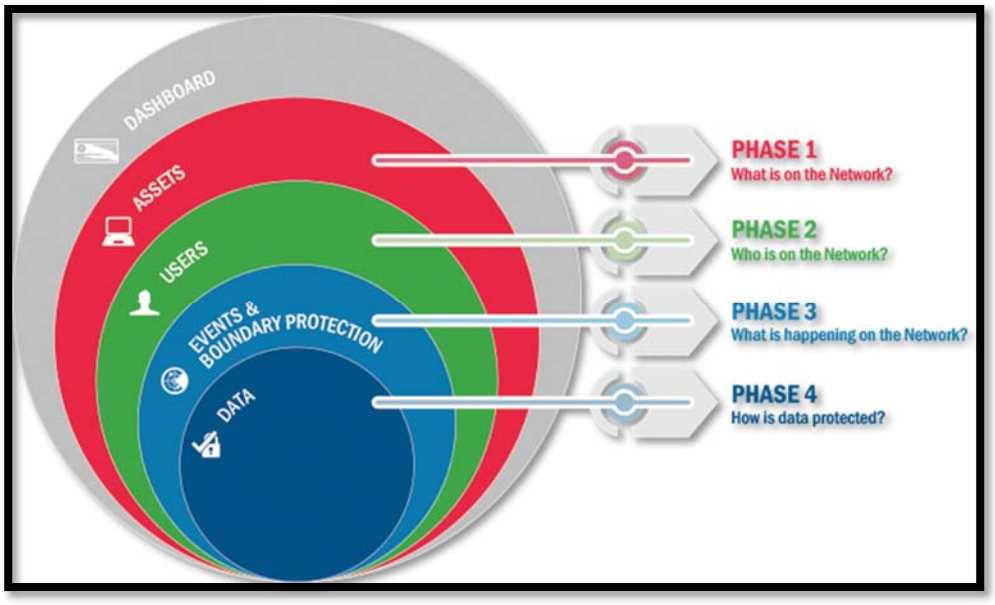
2. Continuous Diagnostics and Mitigation

NCPS's companion program, CDM, provides the "capabilities and tools [to] identify cybersecurity risks on an ongoing basis, prioritize these risks based on potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first."[149] CDM aims to "provide adequate, risk-based, and cost-effective cybersecurity and more efficiently allocate cybersecurity resources."[150]

---

[140] *Id.*
[141] 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 (DEC. 18, 2018).
[142] *Id.*
[143] *Id.* at 34.
[144] *Id.*
[145] *Id.* at 35.
[146] *Id.*
[147] *Id.* at 14.
[148] *Id.*
[149] *Continuous Diagnostics and Mitigation (CDM)*, U.S. Dep't of Homeland Security, https://www.dhs.gov/cdm.
[150] *Id.*

CDM's tools include sensors that carry out automated scans for known vulnerabilities.[151] DHS staff then place the results of these scans on a dashboard that can be accessed by network managers.[152] This dashboard then helps allocate resources for each identified vulnerability.[153] The chart below illustrates the four phases of the CDM program:



[154]

Although DHS has worked to implement several of the phases outlined above, GAO recently concluded that DHS failed to meet the planned implementation dates for each phase.[155] DHS is now in Phase 3 of the implementation process despite the initial projection that this phase would be completed at 97 percent of federal agencies by the end of FY 2017.[156] At present, DHS expects to fully implement Phase 3 in FY 2019.[157]

---

[151] 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 (DEC. 18, 2018).
[152] *Id.*
[153] *Id.*
[154] *Continuous Diagnostics and Mitigation (CDM)*, U.S. Dep't of Homeland Security, US-CERT, https://www.us-cert.gov/cdm/home.
[155] 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 (DEC. 18, 2018).
[156] *Id.* at 38.
[157] *Id.* at 39.

G. OMB Cybersecurity Risk Determination Report

In May 2018, OMB published a Federal Cybersecurity Risk Determination Report and Action Plan in accordance with Executive Order 13800.[158] OMB concluded that the two most significant areas of risk were "the abundance of legacy information technology, which is difficult and expensive to protect, as well as shortages of experienced and capable cybersecurity personnel."[159] Moreover, OMB determined that 71 of 96 agencies, or 74 percent, "participating in the risk assessment process have cybersecurity programs that are either at risk or high risk."[160] Of those 71 agencies, 12 were determined to have cybersecurity programs at high risk.[161] The report then issued four primary findings based upon OMB's risk assessment.[162] Those findings are detailed below.

1. Limited Agency Situational Awareness

First, OMB concluded that federal agencies "do not understand and do not have the resources to combat the current threat environment."[163] OMB's assessment revealed "that those charged with defending agency networks often lack timely information regarding the tactics, techniques, and procedures that threat actors use to exploit government information systems."[164] As evidence of this, OMB found federal agencies could not identify the method of attack in 38 percent of the security incidents "that led to the compromise of information or system functionality in FY 2016."[165] In addition, OMB determined that only 59 percent of agencies had the capability to succinctly communicate cyber risks across their departments.[166]

To address these issues, OMB recommended that agencies adopt the Cyber Threat Framework "which provides decision makers at all levels with the insight and knowledge to make well-informed, prioritized cybersecurity investment decisions."[167] This framework also produces simplified threat information that is more easily transmittable across an agency.[168] In addition to the adoption of the Cyber Threat Framework, OMB recommended that agencies discontinue blind IT

---

[158] OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, FEDERAL CYBERSECURITY RISK DETERMINATION REPORT AND ACTION PLAN, 2 (2018).
[159] *Id.*
[160] *Id.* at 3.
[161] *Id.* at 5.
[162] *Id.* at 3.
[163] *Id.* at 6.
[164] *Id.*
[165] *Id.*
[166] *Id.*
[167] *Id.* at 7.
[168] *Id.*

spending "for perceived security gaps," and instead allocate funds "to address gaps that threat actors are actually exploiting."[169]

2. Lack of Standardized IT Capabilities

Second, OMB determined that "agencies do not have standardized cybersecurity processes and IT capabilities, which impacts their ability to efficiently gain visibility and effectively combat threats."[170] For example, OMB found that agencies often operate numerous email services increasing their susceptibility to phishing attacks.[171] OMB found that one agency had 62 separate email services "making it virtually impossible to track and inspect inbound and outbound communications across the agency."[172] Beyond this, OMB concluded that only 49 percent of agencies have the ability to "whitelist" which "is a process by which agencies list applications and application components that are authorized for use in an organization."[173]

To better monitor phishing activity, OMB recommended that agencies standardize and consolidate their email services to enhance their ability to monitor traffic moving across their network.[174] Doing so also has the added benefit of $1 million to $4 million in annual cost savings.[175] OMB believed that agency whitelisting capabilities will increase as DHS continues to roll out CDM Phase 1.[176]

3. Limited Network Visibility

Third, OMB found that "agencies lack visibility into what is occurring on their networks, and especially lack the ability to detect data exfiltration."[177] In particular, OMB discovered that only 27 percent of agencies have the ability "to detect and investigate attempts to access large volumes of data."[178] This means that currently 73 percent of agencies are unable to tell when large amounts of data are removed from their networks.[179]

To remedy this problem, OMB suggested that agencies "begin consolidating their Security Operations Center ("SOC") capabilities and processes."[180] OMB's assessment found that greater than 70 percent of agencies spend less than $1

---

[169] *Id.* at 8.
[170] *Id.* at 12.
[171] *Id.* at 13.
[172] *Id.*
[173] *Id.* at 14.
[174] *Id.* at 13.
[175] *Id.*
[176] *Id.* at 14.
[177] *Id.* at 15.
[178] *Id.*
[179] *Id.*
[180] *Id.*

million on SOC capabilities indicating that "a significant number of agencies are unable to dedicate the personnel and resources to [defend] themselves from malicious cyber activity."[181]

4. Lack of Accountability for Managing Risks

Fourth, OMB concluded that agencies "lack standardized and enterprise-wide processes for managing cybersecurity risks."[182] FISMA, as well as Executive Order 13800, tasked agency heads with the ultimate responsibility for their organization's information security program.[183] Most agencies have recently reported that "their leadership was actively engaged in cybersecurity risk management."[184] Despite this, many agencies either did not or could not "elaborate in detail on leadership engagement above the CIO level."[185] This is problematic because OMB's assessment showed that CIOs often do not have the authority to make organization-wide information security decisions despite the authorities granted to CIOs in FISMA and FITARA.[186] This results in a lack of senior accountability for cybersecurity risks.[187]

To promote greater senior level accountability, OMB suggested a quarterly reporting process that "tracks quarterly performance against strategic performance targets, communicates the resulting risks to stakeholders, and provides a sense of the return on investment for cybersecurity protections over time."[188]

IV. EXAMPLES OF AGENCY NONCOMPLIANCE

The Subcommittee reviewed the last ten years of FISMA reports published by agency IGs, as FISMA requires. This section summarizes IG reports for seven agencies the Subcommittee believes illustrate the federal government's failure to adhere to information security requirements. The seven agencies highlighted in this report are: the Department of State; the Department of Transportation; the Department of Housing and Urban Development; the Department of Agriculture; the Department of Health and Human Services; the Department of Education; and the Social Security Administration. The Subcommittee reviewed OMB's FY 2017 government-wide FISMA report, and selected these agencies because they had the lowest cybersecurity program ratings based on NIST's cybersecurity framework.

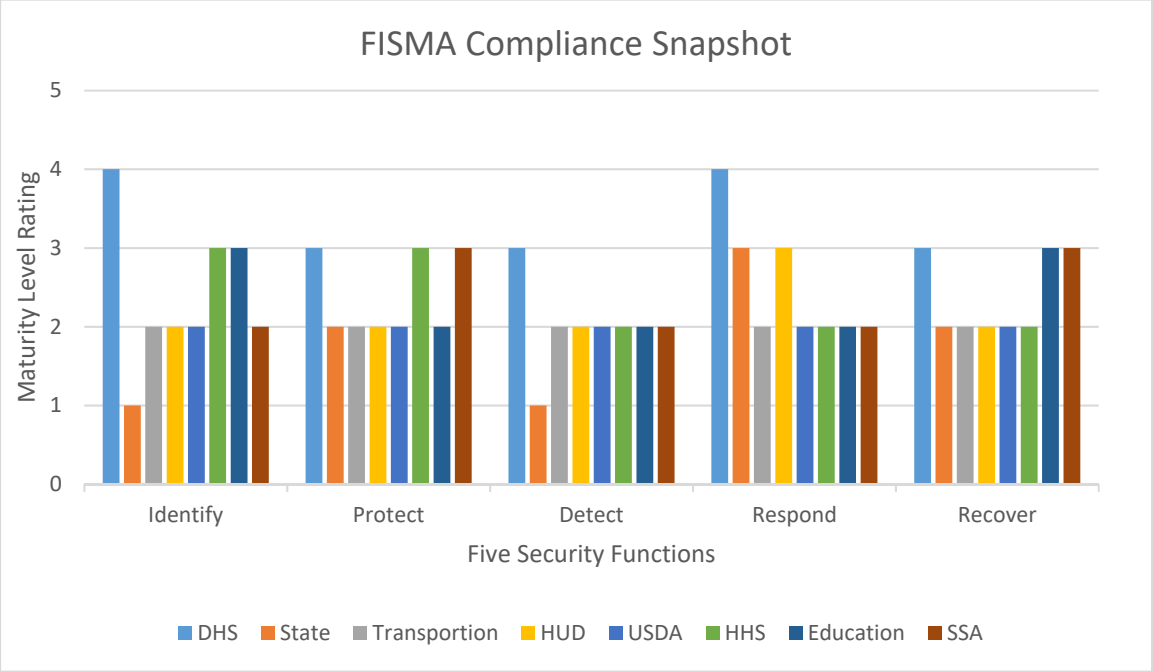
This section also evaluates DHS's compliance with FISMA requirements and the Department's failure to set the government standard for effective information

---

[181] *Id.* at 16.
[182] *Id.* at 17.
[183] *Id.*
[184] *Id.*
[185] *Id.*
[186] *Id.*
[187] *Id.*
[188] *Id.*

security programming. In the more than four years since FISMA's passage, federal agencies have failed to substantially improve their information security posture. The vast majority of the federal government has failed to implement basic and effective data security controls—leaving PII and other sensitive information vulnerable to exploitation.[189]

The chart below provides a snapshot of the information security programs of the agencies mentioned above. Numbers 1 through 5 on the x-axis correspond to the previously mentioned maturity ratings. A rating of 1 signifies an "Ad Hoc" maturity, while 5 represents an "Optimized" rating.[190] Any rating less than 4 is considered ineffective.[191] All agencies listed failed to achieve "Optimized" ratings.



[192]

[189] 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, 19 (DEC. 18, 2018).
[190] OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014: ANNUAL REPORT TO CONGRESS, 26 (2017).
[191] *Id.* at 27.
[192] Office of Inspector General, U.S. Dep't of Homeland Security, OIG 18-56, Evaluation of DHS' Information Security Program for FY 2017, 4 (Mar. 1, 2018); Office of Inspector General, U.S. Dep't of State, AUD-IT-19-08, Audit of the Department of State Information Security Program, 21–24 (Oct. 2018); Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2018017, FISMA 2017: DOT's Information Security Posture Is Still Not Effective, 3 (Jan. 24, 2018); Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2018017, FISMA 2018: DOT's Information Security Posture Is Still Not Effective, Audit Highlights (Mar. 20, 2019); Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2018-OE-0003, HUD Fiscal Year 2018 Federal Information Security Modernization Act 2014 Evaluation Report, 9 (Oct. 31, 2018); Office of Inspector General, U.S. Dep't of Agriculture, 50501-0018-12, Fiscal Year 2018 Federal Information Security Modernization Act, 6 (Oct. 12, 2018); Office of Inspector General, U.S. Dep't of Health &

As shown here, only DHS received an effective, "Managed and Measurable" maturity rating in any one of the five security functions. Collectively, the graph illustrates how agencies failed to implement appropriate information security controls.

The individual agency sections below each highlight: (1) examples of information held by the agency; (2) the agency's failures in the most recent FISMA report; (3) the agency's persistent cybersecurity problems; (4) CIO turnover; and (5) agency IT spending on operations and maintenance. All databases mentioned are examples of the information maintained by that agency and any reference to such a database in this report should not be construed as an example of an agency database that has been compromised.

A. The Department of Homeland Security

The mission of DHS is to ensure that the United States "is safe, secure, and resilient against terrorism and other hazards."[193] In particular, DHS has five core missions: (1) preventing terrorism and enhancing security; (2) securing and managing U.S. borders; (3) enforcing and administering immigration laws; (4) safeguarding and securing cyberspace; and (5) ensuring resilience to disasters.[194]

Despite this mandate, the Department's most recent FISMA audit established that it has yet to comply with its own metrics for what qualifies as an effective information security program.[195] This failure is especially problematic given the Department's administrative duties under FISMA.[196] The Subcommittee's review, however, was based on the DHS IG's FY 2017 FISMA audit. At the time of this report's release, the FY 2018 audit was not available for the Subcommittee to examine.

1. Examples of Information Held by the Department of Homeland Security

As a large agency with over twenty separate components and a diverse mission, DHS holds a significant amount of PII. One example of a DHS database

---

Human Services, A-18-18-11200, Review of the Department of Health and Human Services' Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2018, 4 (Apr. 2019); Office of Inspector General, U.S. Dep't of Education, ED-OIG/A11S0001, The U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report For Fiscal Year 2018, 7 (Oct. 2018); Office of Inspector General, U.S. Social Security Administration, A-14-18-50505, The Social Security Administration's Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2018, 5 (Oct. 31, 2018).

[193] *Our Mission*, U.S. Dep't of Homeland Security, https://www.dhs.gov/our-mission.

[194] *Id.*

[195] Office of Inspector General, U.S. Dep't of Homeland Security, OIG 18-56, Evaluation of DHS' Information Security Program for FY 2017, 4 (Mar. 1, 2018).

[196] Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 44 U.S.C. § 3553(b).

containing PII is Customs and Border Protection's ("CBP") TECS System. CBP uses TECS as its "principal system used by officers at the border to assist with screening and determinations regarding admissibility of arriving persons."[197] As part of this process, CBP collects information such as names, Social Security numbers, dates of birth, addresses, telephone numbers, citizenship information, gender, occupation, and driver's license information.[198]

PII is also heavily involved in CBP's collection of Passenger Name Record ("PNR") data. According to DHS, CBP collects this information "primarily for purposes of preventing, detecting, investigating, and prosecuting terrorist offenses," and gathers it from airline reservations sent to CBP before departure.[199] Examples of the PNR data taken from commercial airlines include dates of reservation, dates of intended travel, names, credit card numbers, travel itinerary, baggage information, and seat number.[200]

Another database under the Department's authority is FEMA's National Flood Insurance Program ("NFIP") PIVOT system. FEMA designed the PIVOT system to help the NFIP validate insurance policies, claims, and data.[201] PIVOT "collects, uses, maintains, retrieves, and disseminates personally identifiable information about individuals who purchase flood insurance programs, those who process insurance policies, and individuals requesting access to the system."[202] Examples of the information collected from policyholders include name, Tax Identification Number, address, email, telephone number, and coverage information.[203]

A fourth DHS database that deals with significant PII is the U.S. Citizenship and Immigration Services' ("USCIS") Citizenship and Immigration Data Repository ("CIDR"). CIDR allows USCIS to vet citizenship applications materials for "possible immigration fraud and national security concerns."[204] Examples of information collected by CIDR include name, immigration status, travel information, marital status, address, telephone number, date of birth, citizenship, and criminal history.[205]

---

[197] U.S. Dep't of Homeland Security, DHS/CBP/PIA-009(a), TECS System: CBP Primary and Secondary Processing National SAR Initiative, 2 (Aug. 5, 2011).
[198] U.S. Dep't of Homeland Security, Privacy Impact Assessment for the TECS System: CBP Primary and Secondary Processing, 8 (Dec. 22, 2010).
[199] U.S. Dep't of Homeland Security, U.S. Customs and Border Protection Passenger Name Record (PNR) Privacy Policy, 1 (Jun. 21, 2013).
[200] *Id.* at 3.
[201] U.S. Dep't of Homeland Security, Privacy Impact Assessment for the National Flood Insurance Program PIVOT System, 1 (Mar. 28, 2018).
[202] *Id.*
[203] *Id.* at 10–11.
[204] U.S. Dep't of Homeland Security, Privacy Impact Assessment for the Citizenship and Immigration Data Repository, 1 (Jan. 3, 2017).
[205] *Id.* at 10–12.

DHS's outstanding cybersecurity vulnerabilities threaten not only the PII entrusted to its care, but also sensitive national security information. A good example of this is the information associated with DHS's Chemical Facility Anti-Terrorism Standards ("CFATS") program.[206] CFATS is managed by DHS's Cybersecurity and Infrastructure Agency and was established to "identify high-risk chemical facilities and assess the risk posed by them; . . . . approve security plans prepared by facilities; and inspect facilities to ensure compliance with regulatory requirements."[207] The security of this information is important given that "thousands of facilities that produce, use, or store hazardous chemicals could be of particular interest to terrorists who might seek to use toxic chemicals to inflict mass casualties in the United States."[208]

2. FY 2017 Inspector General FISMA Report

The DHS IG found that the Department's information security program "fell short of meeting the targeted 'Level 4' for effectiveness in three of five areas listed."[209] Specifically, the IG found that DHS was not effective in the Protect, Detect, and Recover NIST functions. [210]

Lack of Valid Authorities to Operate. This review revealed that 48 unclassified and 16 national security systems did not have valid authority to operate.[211] These authorities are usually granted by DHS for a period of three years.[212] For the systems lacking a valid authority, it means that an "official management decision given by a senior organizational official to authorize the operation of a system and explicitly accept the risk to organizational operations" was not granted.[213] In the absence of updated authorizations, DHS "cannot ensure that its systems are properly secured to protect sensitive information."[214] The Department recently informed the Subcommittee that the Chief Information Security Officer ("CISO") published an Information Security Performance Plan "to

---

[206] 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 (FEB. 27, 2019).
[207] *Id.*
[208] *Id.*
[209] Office of Inspector General, U.S. Dep't of Homeland Security, OIG 18-56, Evaluation of DHS' Information Security Program for FY 2017, 4 (Mar. 1, 2018).
[210] *Id.*
[211] *Id.* at 5.
[212] *Id.* at 6.
[213] *Computer Security Resource Center Glossary*, NAT. INST. OF STANDARDS & TECHNOLOGY, https://csrc.nist.gov/glossary/term/authorization-to-operate.
[214] Office of Inspector General, U.S. Dep't of Homeland Security, OIG 17-24, Evaluation of DHS' Information Security Program for FY 2016, DHS OIG Highlights, 5 (Jan. 18, 2017).

separately monitor ATO of high value assets ("HVA") systems and add additional scoring weight to HVAs for other key categories."[215]

Use of Unsupported Systems. The IG found that DHS continued to use unsupported operating systems creating the possibility that "known or new vulnerabilities [could] be exploited on operating systems for which vendors no longer provide service patches or technical support."[216] For example, the IG determined that several DHS components still used Windows Server 2003—for which Microsoft stopped providing updates in 2015.[217] These components included DHS Headquarters, Coast Guard, and Secret Service.[218] Use of these systems exposes "DHS data to unnecessary security risks" because these systems do not receive security updates to remediate a system's identified vulnerabilities.[219] DHS informed the Subcommittee that it has increased efforts to remove unsupported systems by having the CISO track removals and report the results on monthly FISMA scorecards.[220]

Failure to Remediate Vulnerabilities. During its review, the IG determined that DHS "did not apply security patches timely to mitigate critical and high-risk security vulnerabilities on selected systems."[221] Specifically, the IG found several Windows 8.1 and Windows 7 workstations that did not have patches to protect against WannaCry ransomware "that infected tens of thousands of computers in over 150 countries in May 2017."[222] The failure to address these critical vulnerabilities can result in compromise of DHS data and operations.[223]

3. Persistent Problems Based on Prior IG FISMA Audits

Lack of Valid Authorities to Operate. In every FISMA report since FY 2011, the IG found that DHS operated systems without valid authorizations.[224] In FY

---

[215] Email from U.S. Dep't of Homeland Security to Subcommittee staff (June 7, 2019) (On file with Subcommittee).
[216] Office of Inspector General, U.S. Dep't of Homeland Security, OIG 18-56, Evaluation of DHS' Information Security Program for FY 2017, 11 (Mar. 1, 2018).
[217] *Id.* at 12.
[218] *Id.*
[219] *Id.*; Office of Inspector General, U.S. Dep't of Homeland Security, OIG 17-24, Evaluation of DHS' Information Security Program for FY 2016, DHS OIG Highlights, 5 (Jan. 18, 2017).
[220] Email from U.S. Dep't of Homeland Security to Subcommittee staff (June 7, 2019) (On file with Subcommittee).
[221] Office of Inspector General, U.S. Dep't of Homeland Security, OIG 18-56 (Revised), Evaluation of DHS' Information Security Program for FY 2017, 4, 10 (Mar. 1, 2018).
[222] *Id.* at 13.
[223] *Id.*
[224] Office of Inspector General, U.S. Dep't of Homeland Security, OIG 11-113, Evaluation of DHS' Information Security Program for FY 2011, 6 (Sept. 2011); Office of Inspector General, U.S. Dep't of Homeland Security, OIG 13-04, Evaluation of DHS' Information Security Program for FY 2012, 8 (Oct. 2012); Office of Inspector General, U.S. Dep't of Homeland Security, OIG 14-09, Evaluation of DHS' Information Security Program for FY 2013, 5 (Nov. 2013); Office of Inspector General, U.S. Dep't of Homeland Security, OIG 15-16, Evaluation of DHS' Information Security Program for FY

2015 for instance, DHS "operated 220 'sensitive but unclassified,' 'Secret,' and 'Top Secret' systems with expired authorities to operate."[225] This number dropped to 79 in 2017 and 64 in 2018.[226] Despite that improvement, the number of expired authorizations is still substantial, thereby inhibiting DHS's ability to "ensure that its systems are adequately secured to protect the sensitive information stored and processed in them."[227]

Use of Unsupported Systems. The IG cited DHS's continued use of unsupported operating systems in *four* consecutive FISMA audits beginning in FY 2014.[228] During this time, for example, the IG found FEMA's use of unsupported Windows XP workstations "put FEMA's 'Top Secret' data at risk."[229] In that same fiscal year, the IG reported that DHS was operating an unsupported version of Windows Server 2003 on 3,044 servers.[230] Despite that IG finding in FY 2015, the IG noted that DHS continued to use Microsoft Server 2003 in each of the last two FISMA reports.[231]

Failure to Remediate Vulnerabilities. The IG documented DHS's failure to apply security patches and otherwise remediate security weaknesses in *ten* consecutive FISMA audits.[232] For instance, in FY 2016, the IG discovered

---

2014, 4 (Dec. 12, 2014); Office of Inspector General, U.S. Dep't of Homeland Security, OIG 16-08, Evaluation of DHS' Information Security Program for FY 2015, 9 (Jan. 5, 2016); Office of Inspector General, U.S. Dep't of Homeland Security, OIG 17-24, Evaluation of DHS' Information Security Program for FY 2016, DHS OIG Highlights, 5 (Jan. 18, 2017); Office of Inspector General, U.S. Dep't of Homeland Security, OIG 18-56, Evaluation of DHS' Information Security Program for FY 2017, 5 (Mar. 1, 2018).

[225] Office of Inspector General, U.S. Dep't of Homeland Security, OIG 16-08, Evaluation of DHS' Information Security Program for FY 2015, DHS OIG Highlights (Jan. 5, 2016).

[226] Office of Inspector General, U.S. Dep't of Homeland Security, OIG 17-24, Evaluation of DHS' Information Security Program for FY 2016, DHS OIG Highlights (Jan. 18, 2017); Office of Inspector General, U.S. Dep't of Homeland Security, OIG 18-56, Evaluation of DHS' Information Security Program for FY 2017, DHS OIG Highlights (Mar. 1, 2018).

[227] Office of Inspector General, U.S. Dep't of Homeland Security, OIG 17-24, Evaluation of DHS' Information Security Program for FY 2016, DHS OIG Highlights (Jan. 18, 2017).

[228] Office of Inspector General, U.S. Dep't of Homeland Security, OIG 15-16, Evaluation of DHS' Information Security Program for FY 2014, 17 (Dec. 12, 2014); Office of Inspector General, U.S. Dep't of Homeland Security, OIG 16-08, Evaluation of DHS' Information Security Program for FY 2015, 8,10,20 (Jan. 5, 2016); Office of Inspector General, U.S. Dep't of Homeland Security, OIG 17-24, Evaluation of DHS' Information Security Program for FY 2016, DHS OIG Highlights, 11-12 (Jan. 18, 2017); Office of Inspector General, U.S. Dep't of Homeland Security, OIG 18-56, Evaluation of DHS' Information Security Program for FY 2017, 10,12 (Mar. 1, 2018).

[229] Office of Inspector General, U.S. Dep't of Homeland Security, OIG 16-08, Evaluation of DHS' Information Security Program for FY 2015, 20 (Jan. 5, 2016).

[230] *Id.* at 10.

[231] Office of Inspector General, U.S. Dep't of Homeland Security, OIG 17-24, Evaluation of DHS' Information Security Program for FY 2016, 11 (Jan. 18, 2017); Office of Inspector General, U.S. Dep't of Homeland Security, OIG 18-56, Evaluation of DHS' Information Security Program for FY 2017, 12 (Mar. 1, 2018).

[232] Office of Inspector General, U.S. Dep't of Homeland Security, OIG 08-94, Evaluation of DHS' Information Security Program for FY 2008, 34 (Sept. 2008); Office of Inspector General, U.S. Dep't of Homeland Security, OIG-09-109, Evaluation of DHS' Information Security Program for FY 2009, 12-

numerous missing security patches on Windows 2008 and 2012 operating systems.[233] According to Microsoft, some of the patches were high risk and should have been remediated by August 2012, "while other missing critical patches [that] should have been mitigated dated back to January 2014."[234] In the following fiscal year, the IG once again found missing patches for Windows 2008 and 2012 operating systems, several of which dated back to July 2013.[235] The failure to resolve these high-risk vulnerabilities exposes DHS to the risk of "significant data loss and system disruption, which hampers mission-critical DHS operations."[236]

4. CIO Turnover and OCIO Challenges

Between 2012 and 2017, the median tenure for federal agency CIOs was approximately two years and eight months.[237] Over that same period, only 25 percent of agency CIOs remained in office for at least three years.[238] DHS had six CIOs from 2012 to 2017.[239] The current DHS CIO has been in office for roughly a year and a half after assuming the post in December 2017.[240]

With such consistent CIO turnover, managerial issues have plagued DHS's Office of the Chief Information Officer ("OCIO") for years. In 2013, the McLeod Group reviewed the DHS OCIO and concluded that it had a "toxic organizational culture and low workforce engagement."[241] The McLeod Group report further

---

13 (Sept. 2009); Office of Inspector General, U.S. Dep't of Homeland Security, OIG 11-01, Evaluation of DHS' Information Security Program for FY 2010, 12 (Oct. 2010); Office of Inspector General, U.S. Dep't of Homeland Security, OIG 11-113, Evaluation of DHS' Information Security Program for FY 2011, 1 (Sept. 2011); Office of Inspector General, U.S. Dep't of Homeland Security, OIG 13-04, Evaluation of DHS' Information Security Program for FY 2012, 13 (Oct. 2012); Office of Inspector General, U.S. Dep't of Homeland Security, OIG 14-09, Evaluation of DHS' Information Security Program for FY 2013, 5 (Nov. 2013); Office of Inspector General, U.S. Dep't of Homeland Security, OIG 15-16, Evaluation of DHS' Information Security Program for FY 2014, 18 (Dec. 12, 2014); Office of Inspector General, U.S. Dep't of Homeland Security, OIG 16-08, Evaluation of DHS' Information Security Program for FY 2015, 21 (Jan. 5, 2016); Office of Inspector General, U.S. Dep't of Homeland Security, OIG 17-24, Evaluation of DHS' Information Security Program for FY 2016, DHS OIG Highlights, 12 (Jan. 18, 2017); Office of Inspector General, U.S. Dep't of Homeland Security, OIG 18-56, Evaluation of DHS' Information Security Program for FY 2017, 10 (Mar. 1, 2018).

[233] Office of Inspector General, U.S. Dep't of Homeland Security, OIG 17-24, Evaluation of DHS' Information Security Program for FY 2016, 12 (Jan. 18, 2017).

[234] *Id.*

[235] Office of Inspector General, U.S. Dep't of Homeland Security, OIG 18-56, Evaluation of DHS' Information Security Program for FY 2017, 13 (Mar. 1, 2018).

[236] *Id.*

[237] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 18-93, FEDERAL INFORMATION OFFICERS: CRITICAL ACTIONS NEEDED TO ADDRESS SHORTCOMINGS AND CHALLENGES IN IMPLEMENTING RESPONSIBILITIES, 29 (AUG. 2018).

[238] *Id.* at 66.

[239] *Id.* at 80.

[240] *Dr. John Zangardi*, U.S. Dep't of Homeland Security (Feb. 21, 2018), https://www.dhs.gov/person/dr-john-zangardi.

[241] DHS OCIO 001813.

stated, "OCIO has reached a critical junction where systematic organizational issues, a demoralized workforce, and deteriorated relations between management and staff threaten its core mission capabilities."[242] More recent assessments of the OCIO show that little progress has been made since 2013. In a 2017 interview with the Subcommittee, then-DHS CIO Richard Staropoli commented on the state of the OCIO saying, "You can write this down and quote me, the problem is piss-poor management."[243]

5. IT Spending on Operations and Maintenance ("O&M")

In a 2016 report, GAO determined that "of the more than $80 billion reportedly spent on federal IT in FY 2015, 26 federal agencies spent about $61 billion on O&M."[244] While amount spent on O&M by agencies includes funding for aging legacy systems, the costs associated with the continued operation of legacy systems is not the exclusive source of O&M expenditures.[245] Several years after that GAO report, DHS has yet to depart from significant O&M spending. For instance, DHS submitted a total FY 2018 IT budget request of $6.83 billion.[246] Of that $6.8 billion, DHS requested $5.65 billion for O&M alone—nearly 83 percent of the overall IT budget.[247] DHS informed the Subcommittee that in FY 2018, 9 percent of the Department's total O&M costs were devoted to "systems in the DHS Portfolio that have either an unsupported Operating system or one or more unsupported products."[248] The Department clarified further saying, "Since [DHS] only maintain[s] costs at the system level, [it was] unable to calculate the O&M Costs at a product level."[249]

One example of a legacy system that contributes to DHS's O&M spending is its Immigration and Customs Enforcement Hiring Tracking System. At 39 years old, this system is among the oldest systems in the federal government.[250] The system tracks "current and prior hiring actions and maintains information about

---

[242] DHS OCIO 001817.
[243] Subcommittee Interview of Richard Staropoli (Aug. 16, 2017).
[244] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 16-696T, INFORMATION TECHNOLOGY: FEDERAL AGENCIES NEED TO ADDRESS AGING LEGACY SYSTEMS, 6 (MAY 25, 2016).
[245] U.S. Off. Mgmt. & Budget, Exec. Off. of the President, *An American Budget: Analytical Perspectives Fiscal Year 2019*, 223 (2018); Email from U.S. Gov't Accountability Office to Subcommittee staff (April 9, 2019) (On file with Subcommittee).
[246] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 18-93, FEDERAL INFORMATION OFFICERS: CRITICAL ACTIONS NEEDED TO ADDRESS SHORTCOMINGS AND CHALLENGES IN IMPLEMENTING RESPONSIBILITIES, 80 (AUG. 2018).
[247] *Id.*
[248] Email from U.S. Dep't of Homeland Security to Subcommittee staff (May 29, 2019) (On file with Subcommittee).
[249] *Id.*
[250] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 16-468, INFORMATION TECHNOLOGY: FEDERAL AGENCIES NEED TO ADDRESS AGING LEGACY SYSTEMS, 30 (MAY 2016).

individuals who are selected for vacant positions."[251] Recently, however, DHS has made efforts to modernize this system and subsequently migrated its COBOL mainframe to the cloud.[252] COBOL stands for Common Business Oriented Language and is "a programming language developed in the late 1950s and early 1960s."[253] According to DHS officials, the outdated COBOL mainframe was migrated in September 2017, and then the full system was migrated to the cloud in November 2018.[254]

B. The State Department

The State Department ("State") aims to advance the national interests of the United States and its people.[255] The Department executes this mission by leading "America's foreign policy through diplomacy, advocacy, and assistance."[256]

1. Examples of Information Held by the State Department

The State Department has previously been identified as a top target for foreign government hackers.[257] Just this past September, State's unclassified email system was breached, exposing the PII of some employees.[258] State has a wealth of PII, including employee background investigation information, payroll data, and employee history records.[259]

For example, State's Integrated Personnel Management System ("IPMS") stores personnel information for State Department employees, contractors, and Foreign Service Consular Agents.[260] Some of the information entered into IPMS includes names, Social Security numbers, dates of birth, legal residences, marital statuses, and employee review data.[261]

State also maintains databases containing PII on non-employees. One such database is the Consular Consolidated Database ("CCD"). CCD maintains both "current and archived data from all of the Consular Affairs post databases around

---

[251] *Id.*
[252] Telephone Call with DHS Immigration and Customs Enforcement IT Personnel (Apr. 9, 2019).
[253] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 16-468, INFORMATION TECHNOLOGY: FEDERAL AGENCIES NEED TO ADDRESS AGING LEGACY SYSTEMS, 26 (MAY 2016).
[254] Telephone Call with DHS Immigration and Customs Enforcement IT Personnel (Apr. 9, 2019).
[255] *What is the Mission of the U.S. Department of State*, U.S. Dep't of State, https://www.state.gov/about/about-the-u-s-department-of-state/.
[256] *Id.*
[257] Eric Geller, *State Department warns staff of surge in hacking attempts*, POLITICO, Apr. 12, 2018, https://www.politico.com/story/2018/04/12/state-department-attempted-hacking-warnings-479725.
[258] Eric Geller & Nahal Toosi, *State Department email breach exposed employees' personal information*, POLITICO, Sept. 17, 2018, https://www.politico.com/story/2018/09/17/state-department-email-personal-information-792665.
[259] Briefing with the U.S. Dep't of State, Office of the Inspector General (Nov. 6, 2018).
[260] U.S. Dep't of State, Integrated Personnel Management System Privacy Impact Assessment, (Aug. 2018).
[261] *Id.*

the world."[262] For example, CCD "provides a database solution for centralized visa and American citizen services."[263] Among other things, State distributes this data to interagency partners for visa and passport vetting.[264] The PII stored in CCD includes names, birthdates, Social Security numbers, nationality, medical information, passport information, arrests and convictions, and family information.[265]

A third State database that contains PII is its Defense Export Control and Compliance System ("DECCS"). The Directorate of Defense Trade Controls uses DECCS "to register entities involved in brokering, manufacturing, exporting, or temporarily importing defense articles or defense services enumerated on the U.S. Munitions List."[266] DECCS collects PII including names, addresses, nationality, licenses, and credit card numbers.[267] State uses this information "in the consideration of export control authorizations and associated functions to ensure transactions are consistent with foreign policy and national security."[268]

Beyond PII, State maintains sensitive information pertaining to national security. One example is its Technical Support Working Group ("TSWG") which "coordinates U.S. government-wide technology prototyping under the National Combating Terrorism Research and Development Program."[269] TSWG's mission is "to identify, prioritize, and coordinate interagency and international R&D requirements and to rapidly develop technologies and equipment to meet the high-priority needs of the combating terrorism community."[270] This information is particularly valuable because TSWG "develops new products and capabilities for those on the front lines of the counterterrorism effort."[271]

State also houses sensitive information related to its Blue Lantern program to monitor the use of military hardware, technology, and services provided to foreign nations.[272] This monitoring includes pre-license and post-shipment checks

---

[262] U.S. Dep't of State, Consular Consolidated Database Privacy Impact Assessment 1 (Oct. 2018).
[263] *Id.*
[264] *Id.* at 2.
[265] *Id.* at 3.
[266] U.S. Dep't of State, Privacy Impact Assessment for the Defense Export Control and Compliance System 1(Jan. 2018).
[267] *Id.* at 2.
[268] *Id.* at 7.
[269] *Programs and Initiatives: Technical Support Working Group*, U.S. Dep't of State, https://www.state.gov/bureau-of-counterterrorism-and-countering-violent-extremism-programs-and-initiatives/#TSWG.
[270] *Id.*
[271] *Id.*
[272] *Blue Lantern End-Use Monitoring Program*, U.S. Dep't of State, https://build.export.gov/build/idcplg?IdcService=DOWNLOAD_PUBLIC_FILE&RevisionSelectionMethod=Latest&dDocName=bg_br_083525.

"to inquire with the end user about the specific use and handling of exported articles."[273]

2. FY 2018 Inspector General FISMA Report

The State Department IG contracted with Williams, Adley & Company-DC, LLP ("Williams Adley"), an independent accounting firm, to audit the Department's information security program. In two of the five security functions, Williams Adley gave the State Department a Level 1, "Ad Hoc," maturity rating.[274] An "Ad Hoc" maturity level is the lowest possible rating under NIST standards. The State Department information security program ranked among the worst in the federal government.

Failure to Remediate Vulnerabilities. Williams Adley found that the Department does not currently have the ability to scan their networks to detect rouge devices.[275] In its review of scans conducted by the Department, Williams Adley determined that there were 76 high risk and 500 medium-risk vulnerabilities that were not properly remediated.[276]

Failure to Compile an Accurate and Comprehensive IT Asset Inventory. Among the specific issues noted by Williams Adley was the State Department's failure to maintain an accurate and complete IT systems inventory.[277] State's failure here is due in part to discrepancies surrounding what qualifies as a "FISMA reportable" asset.[278] Agencies are required to develop and maintain an inventory of major systems operated by or under the control of the agency, which the State Department calls FISMA reportable assets.[279] The Department maintains several databases to manage State's IT assets. For example, one list had 646 reportable assets while another only listed 572.[280] According to Williams Adley, State was not able to provide a sufficient explanation for this difference "illustrating the unreliable reporting mechanism currently in place."[281] An agency "cannot have an effective information security program without first identifying the information that

---

[273] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 16-435, SECURITY ASSISTANCE: U.S. GOVERNMENT SHOULD STRENGTHEN END-USE MONITORING AND HUMAN RIGHTS VETTING FOR EGYPT, 27 (APR. 2016).
[274] Office of Inspector General, U.S. Dep't of State, AUD-IT-19-08, Audit of the Department of State Information Security Program, 21–24 (Oct. 2018).
[275] Office of Inspector General, U.S. Dep't of State, AUD-IT-19-08, Audit of the Department of State Information Security Program, 11 (Oct. 2018).
[276] *Id.* at 12.
[277] Office of Inspector General, U.S. Dep't of State, AUD-IT-19-08, Audit of the Department of State Information Security Program, 8 (Oct. 2018).
[278] Briefing with the U.S. Dep't of State, Office of the Inspector General (Nov. 6, 2018).
[279] Email from U.S. Dep't of State Office of Inspector General to Subcommittee staff, (Jun. 6, 2019) (On file with Subcommittee).
[280] Office of Inspector General, U.S. Dep't of State, AUD-IT-19-08, Audit of the Department of State Information Security Program, 8 (Oct. 2018).
[281] *Id.*

the agency needs to protect," and State has continually failed to develop new policies that would promote the development of an accurate IT inventory.[282]

Failure to Provide for the Adequate Protection of PII. Although State is aware that its systems are the constant target of cyber adversaries, in September 2018 hostile actors "gained access to the Department's unclassified email system and exposed PII of Department employees."[283] Following the identification of the breach, State notified those employees who were impacted and offered three years of credit and identity monitoring services.[284] In an alert detailing the incident, State clarified that the breach involved less than one percent of employee inboxes, and that it had "not detected activity of concern in the Department's classified email system."[285]

Additional Cybersecurity Issues at State. Williams Adley noted that the Department "has not fully developed and implemented its organization-wide information security risk management strategy."[286] At present, State has a strategy, but Williams Adley determined that it failed to outline processes for "categorizing risk, developing a risk profile, [and] responding to risk."[287] Moreover, the current risk management strategy also does not discuss how IT personnel are to quantify the seriousness of information security risks and determine whether those risks are acceptable or unacceptable.[288]

Williams Adley further identified organizational deficiencies that have prevented State from achieving an optimal information security posture. As of October 2018, the CIO did not "have sufficient authority to manage IT activities, as provided for in law."[289] Contrary to Executive Order 13800, which required that the CIO have primary authority over the agency's information security program, internal department guidance currently provides that the CIO share this responsibility with the Bureau of Diplomatic Security.[290] As a result of this decentralization, the CIO has been unable to "compel other bureaus, offices, and posts to implement IT controls."[291]

---

[282] *Id.* at 20.
[283] *Id* at 21.
[284] Eric Geller & Nahal Toosi, *State Department email breach exposed employees' personal information*, POLITICO, Sept. 17, 2018, https://www.politico.com/f/?id=00000165-e8b6-df3d-a177-e8ff0b540000.
[285] *Id.*
[286] Office of Inspector General, U.S. Dep't of State, AUD-IT-19-08, Audit of the Department of State Information Security Program, 9 (Oct. 2018).
[287] *Id.*
[288] *Id.* at 10.
[289] *Id.* at 18.
[290] *Id.*
[291] *Id.*

3. Persistent Problems Based on Prior IG FISMA Audits

Lack of Valid Authorities to Operate. From FY 2011 to 2015, auditors noted that State maintained systems lacking a valid authority to operate.[292] In FY 2013, 23 out of 38 classified systems, or 61 percent, "were operating under an expired Authorization to Operate."[293] Auditors concluded that the CIO "did not prioritize tasks to ensure devoted resources identified, documented, and finalized a risk management framework for their information systems."[294] In FY 2018, State improved the number of systems with valid authorities to operate.[295] The percentage of valid authorities for high impact systems increased from 65 percent to 72 percent, and from 46 percent to 72 percent for moderate impact systems.[296]

Failure to Remediate Vulnerabilities. Between FY 2008 and 2018, auditors concluded that State failed to properly apply security patches in *seven* annual FISMA audits.[297] For instance, in FY 2013, 2015, and 2016 auditors noted that the Department had between several hundred and several thousand unmitigated vulnerabilities.[298]

Failure to Compile an Accurate and Comprehensive IT Asset Inventory. Annual FISMA audits recognized State's inability to compile a comprehensive and

---

[292] Office of Inspector General, U.S. Dep't of State, AUD-IT-12-14, Evaluation of the Department of State Information Security Program, 47 (Nov. 2011); Office of Inspector General, U.S. Dep't of State, AUD-IT-13-03, Audit of Department of State Information Security Program, 18 (Nov. 2012); Office of Inspector General, U.S. Dep't of State, AUD-IT-14-03, Audit of Department of State Information Security Program, 5,53 (Nov. 2013); Office of Inspector General, U.S. Dep't of State, AUD-IT-16-16, Audit of Department of State Information Security Program, 10 (Nov. 2015).

[293] Office of Inspector General, U.S. Dep't of State, AUD-IT-14-03, Audit of the Department of State Information Security Program, 53 (Nov. 2013).

[294] *Id.* at 5.

[295] Email from U.S. Dep't of State to Subcommittee staff, (June 7, 2019) (On file with Subcommittee).

[296] *Id.*

[297] Office of Inspector General, U.S. Dep't of State, AUD-IT-11-07, Review of Department of State Information Security Program, 2,10 (Nov. 2010); Office of Inspector General, U.S. Dep't of State, AUD-IT-12-14, Evaluation of the Department of State Information Security Program, 56 (Nov. 2011); Office of Inspector General, U.S. Dep't of State, AUD-IT-13-03, Audit of Department of State Information Security Program, 2,9 (Nov. 2012); Office of Inspector General, U.S. Dep't of State, AUD-IT-14-03, Audit of Department of State Information Security Program, 9,15,52 (Nov. 2013); Office of Inspector General, U.S. Dep't of State, AUD-IT-16-16, Audit of Department of State Information Security Program, 16 (Nov. 2015); Office of Inspector General, U.S. Dep't of State, AUD-IT-17-17, Audit of the Department of State Information Security Program, 11 (Nov. 2016); Office of Inspector General, U.S. Dep't of State, AUD-IT-19-08, Audit of the Department of State Information Security Program, 12 (Oct. 2018).

[298] Office of Inspector General, U.S. Dep't of State, AUD-IT-14-03, Audit of the Department of State Information Security Program, 15 (Nov. 2013); Office of Inspector General, U.S. Dep't of State, AUD-IT-16-16, Audit of the Department of State Information Security Program, 16 (Nov. 2015); Office of Inspector General, U.S. Dep't of State, AUD-IT-17-17, Audit of the Department of State Information Security Program, 11 (Nov. 2016).

accurate IT asset inventory *seven* times since FY 2008.[299] As mentioned above, State has consistently struggled to determine precisely which systems qualify as "FISMA reportable."[300] For example, the Department "did not identify 773 of 3,843 IT assets as either 'FISMA Reportable' or 'non-FISMA Reportable' within" State's official system inventory.[301] Due to the inaccurate information in State's system inventory database, auditors have been unable to "assess the Authorization to Operate status of the Department's information systems."[302]

Failure to Provide for the Adequate Protection of PII. In addition to the September 2018 incident detailed above, the State's difficulty with the adequate protection of PII has been noted in *five* FISMA reports since FY 2008.[303] In FY 2016 for example, State was unable to produce "an accurate inventory of systems that allow access to personally identifiable information."[304] The Department has acknowledged that it is the constant target of cyber adversaries further emphasizing the importance that State implement an effective information security program.[305]

---

[299] Office of Inspector General, U.S. Dep't of State, AUD-IT-08-36, Review of the Information Security Program at the Department of State, 6 (Oct. 2008); Office of Inspector General, U.S. Dep't of State, AUD-IT-11-07, Review of Department of State Information Security Program, 1,5 (Nov. 2010); Office of Inspector General, U.S. Dep't of State, AUD-IT-14-03, Audit of Department of State Information Security Program, 29 (Nov. 2013); Office of Inspector General, U.S. Dep't of State, AUD-IT-16-16, Audit of Department of State Information Security Program, 9 (Nov. 2015); Office of Inspector General, U.S. Dep't of State, AUD-IT-17-17, Audit of the Department of State Information Security Program, 8 (Nov. 2016); Office of Inspector General, U.S. Dep't of State, AUD-IT-18-12, Audit of the Department of State Information Security Program, 7–8 (Oct. 2017); Office of Inspector General, U.S. Dep't of State, AUD-IT-19-08, Audit of the Department of State Information Security Program, 8 (Oct. 2018).

[300] Office of Inspector General, U.S. Dep't of State, AUD-IT-17-17, Audit of the Department of State Information Security Program, 8 (Nov. 2016).

[301] *Id.*

[302] Office of Inspector General, U.S. Dep't of State, AUD-IT-17-17, Audit of the Department of State Information Security Program, 8 (Nov. 2016).

[303] Office of Inspector General, U.S. Dep't of State, AUD-IT-08-36, Review of the Information Security Program at the Department of State, 23 (Oct. 2008); Office of Inspector General, U.S. Dep't of State, AUD-IT-11-07, Review of Department of State Information Security Program, 2 (Nov. 2010); Office of Inspector General, U.S. Dep't of State, AUD-IT-17-17, Audit of the Department of State Information Security Program, 19 (Nov. 2016); Office of Inspector General, U.S. Dep't of State, AUD-IT-18-12, Audit of the Department of State Information Security Program, 22 (Oct. 2017); Office of Inspector General, U.S. Dep't of State, AUD-IT-19-08, Audit of the Department of State Information Security Program, 20 (Oct. 2018).

[304] Office of Inspector General, U.S. Dep't of State, AUD-IT-17-17, Audit of the Department of State Information Security Program, 9 (Nov. 2016).

[305] Office of Inspector General, U.S. Dep't of State, AUD-IT-18-12, Audit of the Department of State Information Security Program, 21 (Oct. 2017).

4. CIO Turnover and OCIO Challenges

Between 2012 and 2017, State had three CIOs.[306] After operating with an acting CIO since December of 2017, State recently named a permanent CIO in March 2019.[307]

In addition, State Department policies fail to address the role of the CIO in several key respects. First, State's policies do not in any way outline the CIO's role in IT strategic planning.[308] Consequently, Department policies contain no detail on how the CIO is to establish goals for improving IT operations or measure the extent to which IT supports agency programs.[309] Second, Department policies only minimally address the CIO's role in assessing the proficiency of State's IT workforce.[310] Consequently, there is presently no explicit role for the CIO in determining whether staff meet IT knowledge and skills requirements.[311]

5. IT Spending on Operations and Maintenance

GAO found that State, like several other agencies throughout the government, spends a majority of its IT dollars on O&M. Out of State's overall $1.9 billion FY 2018 IT budget request, the Department sought approximately $1.5 billion for O&M—roughly 80 percent of State's total IT budget request.[312] State officials told the Subcommittee that for FY 2018, 68 percent of O&M spending was "invested in systems 5 or more years old, which includes some of the Department's major IT systems being 20 years or older."[313] The Department added it plans to invest roughly $878 million to address legacy IT in FY 2019 and FY 2020.[314]

Three outdated State systems that add to O&M spending are its Diversity Visa Information System, Immigration Visa Information System, and Non-Immigrant Visa System. The Diversity Visa Information System tracks and

---

[306] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 18-93, FEDERAL INFORMATION OFFICERS: CRITICAL ACTIONS NEEDED TO ADDRESS SHORTCOMINGS AND CHALLENGES IN IMPLEMENTING RESPONSIBILITIES, 90 (AUG. 2018).
[307] Angus Loten, *Ex-Johnson & Johnson CIO Named State Department IT Chief*, WALL ST. J., Apr. 1, 2019, https://www.wsj.com/articles/ex-johnson-johnson-cio-named-state-department-it-chief-11554138986.
[308] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 18-93, FEDERAL INFORMATION OFFICERS: CRITICAL ACTIONS NEEDED TO ADDRESS SHORTCOMINGS AND CHALLENGES IN IMPLEMENTING RESPONSIBILITIES, 90 (AUG. 2018).
[309] *Id.*
[310] *Id.*
[311] *Id.*
[312] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 18-93, FEDERAL INFORMATION OFFICERS: CRITICAL ACTIONS NEEDED TO ADDRESS SHORTCOMINGS AND CHALLENGES IN IMPLEMENTING RESPONSIBILITIES, 90 (AUG. 2018).
[313] Email from U.S. Dept. of State to Subcommittee staff (May 23, 2019) (On file with Subcommittee).
[314] *Id.*

validates foreign nationals' visa application information.[315] First introduced in the early 1990s, it is approximately 29 years old.[316] The Immigrant Visa System, which processes immigrant visa petitions DHS sends to State, is roughly 25 years old; the Department first operationalized the system in 1994.[317] The Non-Immigrant Visa System, which State first launched in 1995, processes visa applications for temporary travel to the United States.[318]

The Diversity Visa Information system is vulnerable because it relies on software known as PowerBuilder that the vender no longer supports, creating "information security and infrastructure concerns."[319] Although retirement of this system was supposed to begin in 2018, State provided the Subcommittee with an update on those efforts saying:

> Consular Affairs (CA) intends to modernize all three of the systems identified in the May 2016 GAO Report (DVIS, NIV, and IVIS). As part of CA's modernized Immigrant Visa (mIV) processing initiative, CA is currently piloting a replacement capability for IVIS entitled Pre-Immigrant Visa Overseas Technology (PIVOT). Once the pilot has completed, forecasted at the end of calendar year 2020, IVIS will be decommissioned. DVIS and NIV are still in the planning stages for being modernized.[320]

C. The Department of Transportation

The Department of Transportation ("DOT") seeks to ensure "a fast, safe, efficient, accessible and convenient transportation system that meets vital national interests and enhances the quality of life of the American people today, and into the future."[321]

---

[315] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 16-468, INFORMATION TECHNOLOGY: FEDERAL AGENCIES NEED TO ADDRESS AGING LEGACY SYSTEMS, 51 (MAY 2016).
[316] *Id.*
[317] U.S. Dep't of State, Privacy Impact Assessment for the Immigrant VISA Information System (IVIS), (Dec. 2013); U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 16-468, INFORMATION TECHNOLOGY: FEDERAL AGENCIES NEED TO ADDRESS AGING LEGACY SYSTEMS, 47 (MAY 2016).
[318] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 16-468, INFORMATION TECHNOLOGY: FEDERAL AGENCIES NEED TO ADDRESS AGING LEGACY SYSTEMS, 47 (MAY 2016); *DS-160: Online Nonimmigrant Visa Application*, U.S. Dep't of State, https://travel.state.gov/content/travel/en/us-visas/visa-information-resources/forms/ds-160-online-nonimmigrant-visa-application.html.
[319] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 16-468, INFORMATION TECHNOLOGY: FEDERAL AGENCIES NEED TO ADDRESS AGING LEGACY SYSTEMS, 51 (MAY 2016).
[320] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 16-468, INFORMATION TECHNOLOGY: FEDERAL AGENCIES NEED TO ADDRESS AGING LEGACY SYSTEMS, 51 (MAY 2016); Email from U.S. Dept. of State to Subcommittee staff (April 25, 2019) (On file with Subcommittee).
[321] *What We Do,* U.S. Dep't of Transportation, https://www.transportation.gov/about.

1. Examples of Information Held by the Department of Transportation

One example of PII held by DOT is the information the Federal Aviation Administration ("FAA") collects on licensed pilots and their aircraft. This information is housed in the FAA's Airmen/Aircraft Registry Modernization System ("RMS").[322] RMS allows FAA to track airmen "certificate type, class, rating, and limitations issued to an airman."[323] With respect to aircraft, RMS includes information pertaining to "whom the aircraft is registered, aircraft ownership, and legal instruments pertinent to aircraft."[324]

A second DOT database that handles PII is FAA's Pilot Records Database ("PRD"). PRD functions as "a centralized electronic repository of pilot information to access before allowing an individual to begin services as a pilot."[325] To provide this service, PRD collects pilot information such as airman certificates, failed practical tests, closed enforcement actions, and other accidents or incidents.[326]

A third example of a DOT database containing PII is the National Highway Traffic Safety Administration's ("NHTSA") Artemis system. Artemis "collects and stores PII, as necessary, to enable NHTSA to contact consumers and others regarding complaints, and otherwise facilitate the defect investigation and safety recall process."[327] Under most circumstances, potential defect information is collected directly from consumers who reach out to NHTSA.[328] When this occurs, NHTSA staff enters the information directly into Artemis Vehicle Owner Questionnaires ("VOQ").[329] The PII documented in VOQs includes names, email, telephone numbers, address, vehicle information, and incident information.[330]

In addition to PII, DOT houses sensitive information that the FAA uses to issue aircraft airworthiness certificates.[331] The certifications themselves are issued by FAA's Aircraft Certification Service and "include[] more than 1,300 engineers, scientists, inspectors, test pilots and other experts."[332] During the certification process, FAA reviews information including proposed aircraft designs, conducts

---

[322] U.S. Dep't of Transportation, Privacy Impact Assessment Airmen/Aircraft Registry Modernization System, (Aug. 12, 2004).
[323] *Id.*
[324] *Id.*
[325] U.S. Dep't of Transportation, Privacy Impact Assessment Pilot Records Database, 1 (Jan. 23, 2017).
[326] *Id.* at 3.
[327] U.S. Dep't of Transportation, Privacy Impact Assessment Artemis, 1 (May 22, 2015).
[328] *Id.* at 2.
[329] *Id.*
[330] *Id.*
[331] *Airworthiness Certification Overview*, U.S. Dep't of Transportation, Fed. Aviation Admin., https://www.faa.gov/aircraft/air_cert/airworthiness_certification/aw_overview/.
[332] *Id.*

ground and flight tests, and evaluates the airplane to determine required maintenance and operational suitability.[333]

2. FY 2018 Inspector General FISMA Report

The DOT IG reported that DOT's information security program was insufficient in all five NIST function areas.[334] While the IG found that DOT had "formalized and documented its policies," it failed to consistently implement these polices throughout the Department.[335]

Lack of Valid Authorities to Operate. The DOT IG also determined that the Department operates systems with expired authorizations.[336] Out of 471 departmental systems, 61 were operating with expired authorizations.[337] Of those 61 systems, the DOT sub-components with the most expired authorizations were the FAA with 40 and the Federal Motor Carrier Safety Administration with 14.[338] This failure to reauthorize makes it more difficult for agency officials to determine whether particular operating systems represent a risk to the federal government or whether vendors still support their applications.[339] DOT IG staff indicated that having close to 70 expired authorizations is simply too many.[340]

Use of Unsupported Systems. The DOT IG found the FAA still uses Windows 2003 server devices that "are no longer supported and need to be updated."[341] At the time of the review, the IG was unable to identify a DOT plan to address this issue.[342] Following the IG's audit, DOT indicated that it developed a plan of action to update those devices.[343]

Failure to Remediate Vulnerabilities. During its audit, the DOT IG identified departmental weaknesses in patch management.[344] In particular, the IG found that one FAA system was missing "many patches" including "86 critical, 203 High and 352 Medium vulnerabilities, many related to missing security patches."[345] At the

---

[333] *Id.*
[334] Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2018017, FISMA 2018: DOT's Information Security Posture Is Still Not Effective, Audit Highlights (Mar. 20, 2019).
[335] *Id.*
[336] Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2019023, FISMA 2018: DOT's Information Security Program and Practices, 11 (Mar. 20, 2019).
[337] *Id.*
[338] *Id.*
[339] Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2019023, FISMA 2018: DOT's Information Security Program and Practices, 11 (Mar. 20, 2019); Briefing with the U.S. Dep't of Transportation, Office of the Inspector General (Oct. 11, 2018).
[340] Briefing with the U.S. Dep't of Transportation, Office of the Inspector General (Oct. 11, 2018).
[341] Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2019023, FISMA 2018: DOT's Information Security Program and Practices, 45 (Mar. 20, 2019).
[342] *Id.*
[343] *Id.*
[344] *Id.* at 44.
[345] *Id.*

time of the IG's audit, DOT did not have a plan in place to address these patching issues but indicated that it has developed such a plan following the audit.[346]

Failure to Compile an Accurate and Comprehensive IT Asset Inventory. DOT currently lacks a comprehensive and accurate inventory of its information systems.[347] DOT's inventory "does not include accurate counts of its cloud-based systems, contractor systems, or public facing websites."[348] For example, DOT IG found that FAA and FRA "did not correctly categorize 138 systems as contractor-operated."[349] The mislabeling of contractor systems makes "it difficult for DOT to ensure that it has sufficient controls over these systems."[350] DOT IG staff confirmed that the Department should have a process to inventory IT assets and that it can only secure its network once it knows all IT assets currently in use.[351]

Failure to Provide for the Adequate Protection of PII. From a network access standpoint, DOT also has yet to require the use of personal identity verification ("PIV") cards to login to all agency computers.[352] 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."[353] Despite OMB requiring this by 2012, 211 out of 471 DOT systems have not been equipped for PIV card use.[354] Of the roughly 197 operational systems containing PII, approximately 54 currently do not require PIV card authentication.[355] DOT set the internal goal of equipping all agency computers for PIV card use by the end of 2018, but pushed back the deadline to the end of 2019.[356]

The DOT IG's FY 2018 review also documented that the Department's Respond controls "are insufficient."[357] In 2017, the IG found 10 unresolved security incidents "that were over 90 days old" five of which involved PII.[358] The table below summarizes these 10 incidents:

---

[346] *Id.*
[347] *Id.* at 9.
[348] *Id.* at 9-10.
[349] *Id.* at 10.
[350] *Id.*
[351] Briefing with the U.S. Dep't of Transportation, Office of the Inspector General (Oct. 11, 2018).
[352] Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2019023, FISMA 2018: DOT's Information Security Program and Practices, 19 (Mar. 20, 2019).
[353] *Id.*
[354] *Id.* at 11, 19.
[355] *Id.* at 20.
[356] Briefing with the U.S. Dep't of Transportation, Office of the Inspector General (Oct. 11, 2018).
[357] Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2019023, FISMA 2018: DOT's Information Security Program and Practices, 25 (Mar. 20, 2019).
[358] *Id.*

Table 6. Unresolved Incidents Over 90 Days Old

No.	Age	Incident Title	Incident Description	Open Date	Last updated
1	358	PII Incident	Medical records mailed to the wrong address **	8/10/17	8/22/2017
2	358	PII Incident	Potential PII data found on KSN SharePoint site	8/29/17	8/31/2017
3	357	Vulnerability	NCCIC NCATS Cyber vulnerability	9/25/17	9/25/2017
4	350	PII Incident	Release of PII Data **	9/27/17	9/28/2017
5	345	Vulnerability	NCCIC NCATS Cyber vulnerability.	10/3/17	10/3/2017
6	343	Vulnerability	NCCIC NCATS Cyber vulnerability	10/3/17	10/3/2017
7	342	Potential PII	Email address spillage	10/18/17	10/21/2017
8	338	Vulnerability	NCCIC NCATS Cyber vulnerability	11/2/17	11/2/2017
9	324	Vulnerability	NCCIC NCATS Cyber vulnerability	11/15/17	11/15/2017
10	322	PII Incident	Privacy breach in the UAS pilot system **	12/11/17	12/14/2017

* Open incident data retrieved on August 7, 2018.
** Confirmed breach.
Source: OIG analysis of DOT data.

[359]

At DOT, the Cybersecurity Management Center ("CSMC") analyzes all security incidents, categorizes them, and then reports them to US-CERT.[360] Although CSMC is specifically tasked with this responsibility, security incidents remain unresolved in part because "CSMC continues to lack access to all departmental systems."[361] This lack of access creates the risk that security incidents at DOT are not getting reported to US-CERT thereby inhibiting DHS's "ability to ensure that Federal systems and information are secure from compromise."[362]

3. Persistent Problems Based on Prior IG FISMA Audits

Lack of Valid Authorities to Operate. In *nine* out of the last *eleven* fiscal years, the IG found that DOT maintained systems that lack valid authorities to operate.[363] Aside from a slight decrease in FY 2018, DOT has experienced a

[359] *Id.* at 26.
[360] *Id.* at 25.
[361] *Id.* at 26.
[362] *Id.*
[363] Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2011022, Timely Actions Needed to Improve DOT's Cybersecurity, 17 (Nov. 15, 2010); Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2012007, FISMA 2011: Persistent Weaknesses in DOT's Controls Challenge the Protection and Security of Its Information Systems, 12 (Nov. 14, 2011); Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2013014, FISMA 2012: Ongoing Weaknesses Impede DOT's Progress Toward Effective Information Security 12 (Nov. 14, 2012); Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2014006, FISMA 2013: DOT Has Made Progress, But Its Systems Remain Vulnerable to Significant Security Threats, 13 (Nov.

significant increase in the number of systems operating without a valid authorization over the last ten years.[364] For example, in FY 2011, DOT had fewer than 10 systems that lacked current authorizations, but by FY 2017, that number had grown to over 70.[365]

Use of Unsupported Systems. The IG has found DOT systems that are no longer supported in each of the last *two* FISMA audits.[366] For instance, in FY 2017 auditors noted that DOT's Federal Motor Carrier Safety Administration Compliant Hotline Database continues to use versions of Adobe Acrobat that no longer receive updates from the vendor and expose that system to unnecessary risk.[367]

Failure to Remediate Vulnerabilities. With the exception of FY 2014, in *every* fiscal year since 2008, the IG found that DOT failed to remediate security vulnerabilities in a timely fashion.[368] Despite an OMB requirement that agencies

---

22, 2013); Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2015009, FISMA 2014: DOT Has Made Progress But Significant Weaknesses in Its Information Security Remain, 15 (Nov. 14, 2014); Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2016001, FISMA 2015: DOT Has Major Success in PIV Implementation, But Problems Persist in Other Cybersecurity Areas, 21 (Nov. 5, 2015); Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2017008, FISMA 2016: DOT Continues to Make Progress, But the Department's Information Security Posture is Still Not Effective, 8 (Nov. 9, 2016); Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2018017, FISMA 2017: DOT's Information Security Posture Is Still Not Effective, 10 (Jan. 24, 2018); Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2019023, FISMA 2018: DOT's Information Security Program and Practices, 6 (Mar. 20, 2019).

[364] Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2019023, FISMA 2018: DOT's Information Security Program and Practices, 6 (Mar. 20, 2019); Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2018017, FISMA 2017: DOT's Information Security Posture Is Still Not Effective, 10 (Jan. 24, 2018).

[365] Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2018017, FISMA 2017: DOT's Information Security Posture Is Still Not Effective, 10 (Jan. 24, 2018).

[366] Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2018017, FISMA 2017: DOT's Information Security Posture Is Still Not Effective, 52 (Jan. 24, 2018); Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2019023, FISMA 2018: DOT's Information Security Program and Practices, 45 (Mar. 20, 2019);

[367] Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2018017, FISMA 2017: DOT's Information Security Posture Is Still Not Effective, 52 (Jan. 24, 2018).

[368] Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2009003, Audit of Information Security Program, 4 (Oct. 8, 2008); Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2010023, Audit of DOT's Information Security Program and Practices, 3 (Nov. 18, 2009); Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2011022, Timely Actions Needed to Improve DOT's Cybersecurity, 14 (Nov. 15, 2010); Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2012007, FISMA 2011: Persistent Weaknesses in DOT's Controls Challenge the Protection and Security of Its Information Systems, 19 (Nov. 14, 2011); Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2013014, FISMA 2012: Ongoing Weaknesses Impede DOT's Progress Toward Effective Information Security 7–8 (Nov. 14, 2012); Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2014006, FISMA 2013: DOT Has Made Progress, But Its Systems Remain Vulnerable to Significant Security Threats, 8 (Nov. 22, 2013); Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2016001, FISMA 2015: DOT Has Major Success in PIV Implementation, But Problems Persist in Other

develop plans of action to "prioritize weakness remediation based on the seriousness of each weakness," in 2017 the IG found 1,360 plans of action that "had start dates for remediation marked 'to be determined,' indicating that [DOT] had not begun work to resolve the weaknesses."[369] More troubling, however, is that of those 1,360 aforementioned plans of action, 296 were considered high priority and 1,064 were considered medium priority.[370]

Failure to Compile an Accurate & Comprehensive IT Asset Inventory. In *every* fiscal year since 2008, the IG found that DOT failed to compile a complete and accurate IT asset inventory.[371] So, for over ten fiscal years, this lack of progress on such a continuously highlighted issue has inhibited "the Department's ability to monitor its systems' security and [put] the systems at risk for unauthorized access and compromise."[372]

Cybersecurity Areas, 15 (Nov. 5, 2015); Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2017008, FISMA 2016: DOT Continues to Make Progress, But the Department's Information Security Posture is Still Not Effective, 11 (Nov. 9, 2016); Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2018017, FISMA 2017: DOT's Information Security Posture Is Still Not Effective, 13–14 (Jan. 24, 2018); Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2019023, FISMA 2018: DOT's Information Security Program and Practices, 44 (Mar. 20, 2019).

[369] Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2018017, FISMA 2017: DOT's Information Security Posture Is Still Not Effective, 13–14 (Jan. 24, 2018).

[370] *Id.* at 14.

[371] Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2009003, Audit of Information Security Program, 16–17 (Oct. 8, 2008); Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2010023, Audit of DOT's Information Security Program and Practices, 12 (Nov. 18, 2009); Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2011022, Timely Actions Needed to Improve DOT's Cybersecurity, 17 (Nov. 15, 2010); Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2012007, FISMA 2011: Persistent Weaknesses in DOT's Controls Challenge the Protection and Security of Its Information Systems, 14 (Nov. 14, 2011); Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2013014, FISMA 2012: Ongoing Weaknesses Impede DOT's Progress Toward Effective Information Security, 16 (Nov. 14, 2012); Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2014006, FISMA 2013: DOT Has Made Progress, But Its Systems Remain Vulnerable to Significant Security Threats, 19 (Nov. 22, 2013); Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2015009, FISMA 2014: DOT Has Made Progress But Significant Weaknesses in Its Information Security Remain, 25 (Nov. 14, 2014); Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2016001, FISMA 2015: DOT Has Major Success in PIV Implementation, But Problems Persist in Other Cybersecurity Areas, 12–13 (Nov. 5, 2015); Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2017008, FISMA 2016: DOT Continues to Make Progress, But the Department's Information Security Posture is Still Not Effective, 20 (Nov. 9, 2016); Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2018017, FISMA 2017: DOT's Information Security Posture Is Still Not Effective, 21 (Jan. 24, 2018); Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2019023, FISMA 2018: DOT's Information Security Program and Practices, 9 (Mar. 20, 2019).

[372] Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2018017, FISMA 2017: DOT's Information Security Posture Is Still Not Effective, 22 (Jan. 24, 2018).

Failure to Provide for the Adequate Protection of PII. The IG highlighted DOT's inadequate security of PII *six* times over the past eleven fiscal years.[373] DOT's struggle in this regard largely stems from its inability to comply with OMB's requirement that all agencies implement PIV cards for employer and contractor access to departmental facilities.[374] This issue reached its peak in 2016, when the IG found 140 systems containing PII that were not equipped for PIV card use.[375]

4. CIO Turnover and OCIO Challenges

DOT experienced consistent CIO turnover from 2012 to 2017. Over this timespan, DOT has had five CIOs.[376] DOT's current CIO started in February 2019.[377]

This turnover has created challenges within the OCIO, as highlighted by a 2017 DOT IG report that found DOT does not adequately plan for near-term cybersecurity funding needs.[378] This report indicated that inadequate management within the OCIO hindered DOT's ability to comply with OMB requirements for managing investments.[379] In particular, OCIO officials failed to properly oversee, plan, guide, or document processes related to cybersecurity projects.[380] Moreover, the IG found that the Department failed to provide adequate cost-estimate or planning documentation to OMB in support of budget requests, and was not

---

[373] Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2009003, Audit of Information Security Program, 4, 7–8 (Oct. 8, 2008); Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2010023, Audit of DOT's Information Security Program and Practices, 15 (Nov. 18, 2009); Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2011022, Timely Actions Needed to Improve DOT's Cybersecurity, 25 (Nov. 15, 2010); Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2017008, FISMA 2016: DOT Continues to Make Progress, But the Department's Information Security Posture is Still Not Effective, 14–15 (Nov. 9, 2016); Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2018017, FISMA 2017: DOT's Information Security Posture Is Still Not Effective, 18 (Jan. 24, 2018); Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2019023, FISMA 2018: DOT's Information Security Program and Practices, 20 (Mar. 20, 2019).

[374] Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2019023, FISMA 2018: DOT's Information Security Program and Practices, 19 (Mar. 20, 2019);

[375] Office of Inspector General, U.S. Dep't of Transportation, Report No. FI2017008, FISMA 2016: DOT Continues to Make Progress, But the Department's Information Security Posture is Still Not Effective, 15 (Nov. 9, 2016)

[376] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 18-93, FEDERAL INFORMATION OFFICERS: CRITICAL ACTIONS NEEDED TO ADDRESS SHORTCOMINGS AND CHALLENGES IN IMPLEMENTING RESPONSIBILITIES, 92 (AUG. 2018).

[377] Email from U.S. Dep't of Transportation to Subcommittee staff (Jun. 7, 2019) (On file with Subcommittee).

[378] Office of the Inspector General, U.S. Dep't of Transportation, Report No. FI2017066, Audit Report: Cybersecurity Planning Weaknesses May Hinder the Efficient Use of Future Resources, 2 (Aug. 7, 2017).

[379] *Id.*

[380] *Id.*

following OMB or DOT planning guidance for IT investments.[381] The collective impact of this mismanagement is that DOT may not obtain OMB approval for future cybersecurity improvement programs and may provide incomplete information to Congress as well as internal DOT decision makers.[382]

5. IT Spending on Operations and Maintenance

As IT spending is concerned, DOT's FY 2018 IT budget request was roughly $3.2 billion, with the expectation that it would spend $1.5 billion on O&M.[383] While DOT allocates less for O&M than many federal agencies, it still was approximately 47 percent of the overall agency IT budget request. For FY 2018, Department officials estimated that approximately 9.4 percent of O&M spending was specifically devoted to the maintenance of legacy systems.[384]

A particularly outdated DOT legacy system contributing to DOT's O&M budget was its Hazardous Materials Information System—a 48-year-old system.[385] The system "provides access to comprehensive information on hazardous materials incidents, exemptions and approvals, enforcement actions, and other elements that support the regulatory program."[386] Officials from Pipeline and Hazardous Material Safety's Office of the Chief Information Officer noted that maintenance of the system became particularly costly "due to maintaining the personnel with the knowledge to use these older applications."[387] Nevertheless, and since 2016, DOT has made progress replacing the legacy modules of this system and notes that it was decommissioned on May 31, 2019.[388]

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."[389] HUD also works to "strengthen the housing market to bolster the economy

---

[381] *Id.* at 7–12.
[382] *Id.* at 11.
[383] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 18-93, FEDERAL INFORMATION OFFICERS: CRITICAL ACTIONS NEEDED TO ADDRESS SHORTCOMINGS AND CHALLENGES IN IMPLEMENTING RESPONSIBILITIES, 92 (AUG. 2018).
[384] Email from U.S. Dep't of Transportation to Subcommittee staff (May 15, 2019) (On file with Subcommittee).
[385] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 16-468, INFORMATION TECHNOLOGY: FEDERAL AGENCIES NEED TO ADDRESS AGING LEGACY SYSTEMS, 29, 52 (MAY 2016).
[386] *Id.*
[387] *Id.*
[388] Email from U.S. Dep't of Transportation to Subcommittee staff (April 4, 2019) (On file with Subcommittee).
[389] *Mission*, U.S. Dep't of Housing & Urban Development, https://www.hud.gov/about/mission.

and protect consumers [and] utilize housing as a platform for improving quality of life."[390]

1. Examples of Information Held by the Department of Housing and Urban Development

HUD holds roughly 1 billion files containing Americans' PII.[391] The IG noted that a PII breach would be extremely expensive to remediate with the average cost per record lost ranging from $128–$156.[392] Several examples of HUD databases that serve as PII repositories include the Tenant Rental Assistance Certification System and the Enterprise Income Verification System, as discussed below.

The Tenant Rental Assistance Certification System ("TRACS") serves as "the official repository for HUD's Multifamily Housing's assisted families including both current and historical data."[393] HUD employees enter the PII into TRACS with the goal of improving "fiscal control over Section 8 and other assisted housing programs at HUD."[394] The PII collected as part of this process includes names, Social Security numbers, dates of birth, addresses, ethnicity, gender, spousal information, number of children, income, employment history, and disabilities.[395] HUD then uses this information to confirm the eligibility of a tenant as well as the accuracy of that tenant's corresponding subsidy payment.[396]

The Enterprise Income Verification ("EIV") system actually pulls information from TRACS and also "contains employment and income information on individuals participating in HUD's rental assistance programs."[397] Consequently, the PII collected in EIV is similar to the information housed in TRACS.[398] This PII helps HUD to ensure that "the right rental assistance benefits go to the right persons."[399]

---

[390] *Id.*
[391] Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2018-OE-0003, HUD Fiscal Year 2018 Federal Information Security Modernization Act 2014 Evaluation Report, 4 (Oct. 31, 2018).
[392] *Id.*
[393] U.S. Dep't of Housing & Urban Development, Tenant Rental Assistance Certification System Privacy Impact Assessment, 7 (Apr. 2009).
[394] *Id.*
[395] *Id.* at 8.
[396] *Id.* at 7.
[397] U.S. Dep't of Housing & Urban Development, Enterprise Income Verification System Privacy Impact Assessment, 2 (Oct. 5, 2017).
[398] *Id.* at 6–11.
[399] *Id.* at 2.

2. FY 2018 Inspector General FISMA Report

The HUD IG determined that the Department maintained weaknesses in all five NIST security functions.[400] The IG also noted that some key IT positions within the Department have remained vacant since 2014.[401] Furthermore, HUD's CIO has changed four times in the last five years.[402]

Lack of Valid Authorities to Operate. During its review, the HUD IG determined that, unbeknownst to the OCIO, the official HUD website application was not properly authorized to operate.[403] The IG also found that this web application was "using an unapproved government domain" in violation of the requirement that all government URLs use a .gov domain.[404]

Use of Unsupported Systems. HUD operates a number of legacy systems that are increasingly difficult to configure—at least two of these systems have mainframes that date back to the 1980s.[405] Extensive use of legacy systems is not only precarious from a security standpoint, but can be costly to maintain.[406] HUD only designates roughly five percent of its overall IT budget for information security, and the majority of these funds are being devoted to the maintenance of legacy systems instead of modernization efforts.[407]

Failure to Remediate Vulnerabilities. In what is a reoccurring finding, the IG noted that the Department needs to "update and fully document their patch management policy."[408] Specifically, the IG found that the policy lacked detail in "providing direction on timelines for patch management."[409] Likewise, some HUD contractors had their own patch management policies, indicating that HUD has yet to standardize a single policy across the Department.[410]

---

[400] Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2018-OE-0003, HUD Fiscal Year 2018 Federal Information Security Modernization Act 2014 Evaluation Report, 9 (Oct. 31, 2018).
[401] Briefing with the U.S. Dep't of Housing & Urban Development, Office of Inspector General (Oct. 2, 2018).
[402] *Id.*
[403] Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2018-OE-0003, HUD Fiscal Year 2018 Federal Information Security Modernization Act 2014 Evaluation Report, 10 (Oct. 31, 2018).
[404] *Id.*
[405] Briefing with the U.S. Dep't of Housing & Urban Development, Office of Inspector General (Oct. 2, 2018).
[406] *Id.*
[407] *Id.*
[408] Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2018-OE-0003, HUD Fiscal Year 2018 Federal Information Security Modernization Act 2014 Evaluation Report, 44 (Oct. 31, 2018).
[409] *Id.* at 15.
[410] Briefing with the U.S. Dep't of Housing & Urban Development, Office of Inspector General (Oct. 2, 2018).

Failure to Compile an Accurate and Comprehensive IT Asset Inventory. Although HUD compiled an inventory of its IT systems, it was neither comprehensive nor accurate.[411] A 2017 scan revealed that HUD had thousands of software applications on its network.[412] To manage these applications, HUD's Change Control Management Board maintains a list of approved licenses, which should closely mirror the number of applications across their network.[413] Nevertheless, the IG determined that "thousands of software titles did not match" those listed in the software inventory.[414] In the absence of an accurate and comprehensive inventory, security personnel will be unable to apply the security measures necessary to protect the network and data from the threats of hostile actors.[415]

Failure to Provide for the Adequate Protection of PII. HUD currently lacks a defined "process to identify and inventory all of its PII and thus [cannot] review and remove unnecessary PII collections on a regular basis."[416] As a result, the IG discovered that some records were retained in violation of National Archives and Records Administration requirements.[417]

PII is also susceptible to exploitation because the Department does not have a mature process for monitoring network and web application data exfiltration.[418] This is an issue because the IG identified several web applications that allow users to generate reports containing PII.[419] Without routine monitoring of these applications, HUD is less likely to detect the outbound communications traffic indicative of exfiltration.[420]

3. Persistent Problems Based on Prior IG FISMA Audits

Lack of Valid Authorities to Operate. The IG found that HUD operated systems without a valid authority to operate in *four* audits since fiscal year 2008.[421]

---

[411] Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2018-OE-0003, HUD Fiscal Year 2018 Federal Information Security Modernization Act 2014 Evaluation Report, 10 (Oct. 31, 2018).
[412] *Id.* at 11.
[413] *Id.*
[414] *Id.*
[415] *Id.* at 10.
[416] *Id.* at 21.
[417] *Id.*
[418] *Id.* at 22.
[419] *Id.*
[420] *Id.*
[421] Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2013-DP-0006, HUD's Fiscal Year 2012 Information Security Program, 11 (Sept. 12, 2013); Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2013-ITED-0001, Federal Information Security Management Act Fiscal Year 2013 Evaluation Report, 7, 10 (Nov. 29, 2013); Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2014-OE-0003, Federal Information Security Management Act Fiscal Year 2014 Evaluation Report, 65 (Nov. 14, 2014); Office of Inspector

For instance, in FY 2013, the IG determined that ten of the twelve systems reviewed lacked a valid authority to operate.[422] According to the IG, this "means a senior agency official has not accepted accountability for the system."[423]

Use of Unsupported Systems. Since FY 2008, the IG has noted HUD's use of unsupported systems in *seven* FISMA audits—including every year since FY 2013.[424] Although HUD has now acknowledged its excessive reliance upon legacy systems, it continues to use "systems [that] have been in place for decades."[425] Over this timespan, system personnel "report that the status of their legacy application and potential impacts from system failure 'keep them up at night.'"[426]

Failure to Remediate Vulnerabilities. For *seven* consecutive fiscal years, the IG found that HUD did not have a mature process to ensure consistent patch management.[427] Among the issues the IG repeatedly highlighted is that HUD

General, U.S. Dep't of Housing & Urban Development, 2018-OE-0003, HUD Fiscal Year 2018 Federal Information Security Modernization Act 2014 Evaluation Report, 10 (Oct. 31, 2018).

[422] Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2013-ITED-0001, Federal Information Security Management Act Fiscal Year 2013 Evaluation Report, 7 (Nov. 29, 2013).

[423] *Id.*

[424] Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2008-DP-0802, OIG Response to Questions from OMB under the Federal Information Security Management Act of 2002, 3 (Sept. 30, 2008); Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2013-ITED-0001, Federal Information Security Management Act Fiscal Year 2013 Evaluation Report, 6, 10, 18 (Nov. 29, 2013); Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2014-OE-0003, Federal Information Security Management Act Fiscal Year 2014 Evaluation Report, 3 (Nov. 14, 2014); Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2015-OE-0001, HUD Fiscal Year 2015 FISMA Evaluation Report, 31 (2015); Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2016-OE-0006, HUD Fiscal Year 2016 Federal Information Security Modernization Act 2014 Evaluation Report, 32 (Nov. 10, 2016); Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2017-OE-0007, HUD Fiscal Year 2017 Federal Information Security Modernization Act 2014 Evaluation Report, 5 (Oct. 31, 2017); Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2018-OE-0003, HUD Fiscal Year 2018 Federal Information Security Modernization Act 2014 Evaluation Report, 4 (Oct. 31, 2018).

[425] Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2017-OE-0007, HUD Fiscal Year 2017 Federal Information Security Modernization Act 2014 Evaluation Report, 5 (Oct. 31, 2017)

[426] Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2014-OE-0003, Federal Information Security Management Act Fiscal Year 2014 Evaluation Report, 34 (Nov. 14, 2014).

[427] Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2013-DP-0006, HUD's Fiscal Year 2012 Information Security Program, 5 (Sept. 12, 2013); Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2013-ITED-0001, Federal Information Security Management Act Fiscal Year 2013 Evaluation Report, 16–17 (Nov. 29, 2013); Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2014-OE-0003, Federal Information Security Management Act Fiscal Year 2014 Evaluation Report, 4 (Nov. 14, 2014); Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2015-OE-0001, HUD Fiscal Year 2015 FISMA Evaluation Report, 11 (2015); Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2016-OE-0006, HUD Fiscal Year 2016 Federal Information Security Modernization Act 2014 Evaluation Report, 18 (Nov. 10, 2016); Office of Inspector General, U.S. Dep't of Housing &

contractors maintained their own patch management policies "that did not always coordinate or create efficient results."[428] Moreover, the IG reported that contractor policies do not always comply with the OMB and DHS requirements that agencies address critical patches within 30 days.[429]

Failure to Compile an Accurate & Comprehensive IT Asset Inventory. Since FY 2008, the IG has highlighted HUD's failure to compile an accurate IT asset inventory *eight* times.[430] According to the IG, "an accurate inventory of IT systems, interconnections, and software and hardware assets are critical foundational elements for managing risk."[431] To date, HUD has struggled to develop an effective process for the tracking of its systems.[432] For instance, in FY 2017 the IG found that HUD "had no identifiable process to track its inventory of applications and was dependent on program offices to inform it of applications hosted on third-party systems."[433]

Failure to Provide for the Adequate Protection of PII. In *nine* of the last *eleven* fiscal years, the IG found that HUD failed to institute policies that

---

Urban Development, 2017-OE-0007, HUD Fiscal Year 2017 Federal Information Security Modernization Act 2014 Evaluation Report, 13–14 (Oct. 31, 2017); Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2018-OE-0003, HUD Fiscal Year 2018 Federal Information Security Modernization Act 2014 Evaluation Report, 44 (Oct. 31, 2018).

[428] Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2017-OE-0007, Inspector General Section Report: 2017 Annual FISMA Report, 12 (Oct. 31, 2017)

[429] *Id.*

[430] Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2008-DP-0802, OIG Response to Questions from OMB under the Federal Information Security Management Act of 2002, 3 (Sept. 30, 2008); Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2010-DP-0802, OIG Response to Questions from OMB under the Federal Information Security Management Act of 2002, 3 (Nov. 13, 2009); Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2013-ITED-0001, Federal Information Security Management Act Fiscal Year 2013 Evaluation Report, 7 (Nov. 29, 2013); Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2014-OE-0003, Federal Information Security Management Act Fiscal Year 2014 Evaluation Report, 4 (Nov. 14, 2014); Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2015-OE-0001, HUD Fiscal Year 2015 FISMA Evaluation Report, 16 (2015); Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2016-OE-0006, HUD Fiscal Year 2016 Federal Information Security Modernization Act 2014 Evaluation Report, 12 (Nov. 10, 2016); Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2017-OE-0007, HUD Fiscal Year 2017 Federal Information Security Modernization Act 2014 Evaluation Report, 10, 11 (Oct. 31, 2017); Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2018-OE-0003, HUD Fiscal Year 2018 Federal Information Security Modernization Act 2014 Evaluation Report, 10 (Oct. 31, 2018).

[431] Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2017-OE-0007, HUD Fiscal Year 2017 Federal Information Security Modernization Act 2014 Evaluation Report, 11 (Oct. 31, 2017)

[432] Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2014-OE-0003, Federal Information Security Management Act Fiscal Year 2014 Evaluation Report, 20 (Nov. 14, 2014).

[433] Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2017-OE-0007, HUD Fiscal Year 2017 Federal Information Security Modernization Act 2014 Evaluation Report, 11 (Oct. 31, 2017)

adequately protected PII.[434] The Department's shortcomings in this area include the lack of a strategic plan for privacy, unknown PII inventory, inadequate privacy training, and inadequate incident response.[435] HUD's continued lack of progress in implementing these protections "could result in a lack of trust and unwillingness by external parties to share PII data, thereby jeopardizing HUD's ability to complete its mission."[436]

4. CIO Turnover and OCIO Challenges

From 2012 to 2017, HUD had six different CIOs.[437] The current CIO has been in office since August 2018.[438]

In the past, the HUD OCIO has struggled to achieve operational efficiency and cost-savings with respect to IT management.[439] For example, in 2014, GAO determined that HUD established a hierarchy of investment review boards, but failed to outline policies and procedures for these review boards.[440] As a result, the

---

[434] Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2008-DP-0802, OIG Response to Questions from OMB under the Federal Information Security Management Act of 2002, 3 (Sept. 30, 2008); Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2010-DP-0802, OIG Response to Questions from OMB under the Federal Information Security Management Act of 2002, 3 (Nov. 13, 2009); Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2011-DP-0005, Although HUD Continued To Make Improvements to Its Entitywide Security Program, Challenges Remained in Its Efforts to Comply with Federal Information Security Requirements, 9 (Feb. 10, 2011); Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2013-ITED-0001, Federal Information Security Management Act Fiscal Year 2013 Evaluation Report, 9 (Nov. 29, 2013); Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2014-OE-0003, Federal Information Security Management Act Fiscal Year 2014 Evaluation Report, 23, 36 (Nov. 14, 2014); Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2015-OE-0001, HUD Fiscal Year 2015 FISMA Evaluation Report, 1, 15 (2015); Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2016-OE-0006, HUD Fiscal Year 2016 Federal Information Security Modernization Act 2014 Evaluation Report, 40–41, 47 (Nov. 10, 2016); Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2017-OE-0007, HUD Fiscal Year 2017 Federal Information Security Modernization Act 2014 Evaluation Report, 30–31, 36 (Oct. 31, 2017); Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2018-OE-0003, HUD Fiscal Year 2018 Federal Information Security Modernization Act 2014 Evaluation Report, 21 (Oct. 31, 2018).

[435] Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2014-OE-0003, Federal Information Security Management Act Fiscal Year 2014 Evaluation Report, 36 (Nov. 14, 2014).

[436] Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2013-ITED-0001, Federal Information Security Management Act Fiscal Year 2013 Evaluation Report, 9 (Nov. 29, 2013).

[437] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 18-93, FEDERAL INFORMATION OFFICERS: CRITICAL ACTIONS NEEDED TO ADDRESS SHORTCOMINGS AND CHALLENGES IN IMPLEMENTING RESPONSIBILITIES, 82 (AUG. 2018).

[438] Adam Mazmanian, *HUD names new CIO*, FEDERAL COMPUTER WEEK, Aug. 24, 2018, https://fcw.com/articles/2018/08/24/chow-hud-new-cio.aspx.

[439] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 15-56, INFORMATION TECHNOLOGY: HUD CAN TAKE ADDITIONAL ACTIONS TO IMPROVE ITS GOVERNANCE, 26 (DEC. 2014).

[440] *Id.* at 14–15.

review boards failed to meet on a regular basis, did not establish criteria for reviewing investments, and were not assessing their portfolio investments according to the correct priorities.[441] According to GAO, one explanation for these failures was the then-Deputy Secretary's preference for unilaterally deciding IT priorities and hand-selecting individuals to participate in decision-making discussions.[442] HUD later attributed these shortcomings to "changes in leadership, priorities, and approaches."[443]

A more recent IT management challenge at HUD is the Indian Home Loan Guarantee Program's information technology system. Although HUD spent $4 million to develop this system and another $1 million annually in maintenance costs, it still "does not satisfy all management and oversight objectives."[444] Specifically, only 1 of 38 lenders who participate in the program is able to access this system "due to an internal HUD system access issue."[445]

5. IT Spending on Operations and Maintenance

According to GAO, HUD estimated that it would spend $335 million out of its total $351 million FY 2018 IT budget request on O&M.[446] That constitutes 95 percent of HUD's overall IT budget request—the highest percentage of the federal agencies examined in this report. HUD informed the Subcommittee it spends roughly $35 million on the maintenance of legacy systems.[447] This accounts for approximately 13 percent of HUD's overall IT budget.[448]

A legacy system that is part of HUD's O&M spending is its Computerized Homes Underwriting Management System ("CHUMS") which was first introduced in 1984.[449] HUD uses CHUMS "to initiate and track loan case numbers and associated data."[450] In practice, "this system does not interface with HUD's general

---

[441] *Id.*
[442] *Id.* at 14.
[443] *Id.* at Highlights of GAO-15-56.
[444] Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2018-OE-0004, HUD OIG Report: IT System Management and Oversight of the Section 184 Program, 2 (Aug. 13, 2018); Briefing with the U.S. Dep't of Housing & Urban Development, Office of Inspector General (Oct. 2, 2018).
[445] Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2018-OE-0004, HUD OIG Report: IT System Management and Oversight of the Section 184 Program, 4 (Aug. 13, 2018).
[446] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 18-93, FEDERAL INFORMATION OFFICERS: CRITICAL ACTIONS NEEDED TO ADDRESS SHORTCOMINGS AND CHALLENGES IN IMPLEMENTING RESPONSIBILITIES, 82 (AUG. 2018).
[447] Email from U.S. Dept. of Housing & Urban Development to Subcommittee staff (May 31, 2019) (On file with Subcommittee).
[448] *Id.*
[449] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 16-656, FINANCIAL MANAGEMENT SYSTEMS: HUD NEEDS TO ADDRESS MANAGEMENT AND GOVERNANCE WEAKNESSES THAT JEOPARDIZE ITS MODERNIZATION EFFORTS, 49 (JULY 2016).
[450] Office of Inspector General, U.S. Dep't of Housing & Urban Development, 2018-OE-0004, HUD OIG Report: IT System Management and Oversight of the Section 184 Program, 4 (Aug. 13, 2018).

ledger system and requires the lenders to submit loan applications documents to HUD in paper form through regular mail."[451]

E. The Department of Agriculture

The Department of Agriculture ("USDA") works "to promote economic opportunity through innovation, to promote agriculture production that better nourishes Americans, and to preserve our Nation's natural resources through conservation."[452]

1. Examples of Information Held by the Department of Agriculture

USDA has sensitive information including employment records and Social Security numbers.[453] USDA also maintains databases with market sensitive farm commodity information and laboratories that house information on various diseases that could potentially impact agricultural products.[454] The wrongful disclosure of either has the potential to cause serious economic harm to American taxpayers.

One example of a PII-rich USDA database is the Farm Service Agency's ("FSA") Direct Loan System ("DLS"). The DLS "is a web-based application that provides field offices with the ability to process loan applications."[455] Data used in the application review process includes names, Social Security numbers, financial information, loan information, farm production information, liabilities, and assets owned.[456] FSA consults this information when it processes loan applications and responds to existing customer inquiries.[457]

Outside of PII, USDA has sensitive information pertaining to its participation in the Select Agent Program.[458] Hazardous pathogens and toxins "are designated as select agents because they have the potential to pose a severe threat to human, animal, or plant health and safety, or to animal or plant products."[459] Research is conducted on select agents "to identify their characteristics and develop vaccines and other measures to help diagnose, prevent, or treat exposure to these agents."[460] In its split authority with HHS under this program, USDA "is

---

[451] *Id.*
[452] *About the U.S. Dep't of Agriculture*, U.S. Dep't of Agriculture, https://www.usda.gov/our-agency/about-usda.
[453] Briefing with the U.S. Dep't of Agriculture, Office of Inspector General (Nov. 20, 2018).
[454] *Id.*
[455] U.S. Dep't of Agriculture, Privacy Impact Assessment Direct Loan System, (Jun. 30, 2009).
[456] *Id.*
[457] *Id.*
[458] 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, 9 (OCT. 2017).
[459] *Id.* at 3.
[460] *Id.*

responsible for the oversight and regulation of select agents that could pose a threat to animal or plant health or animal or plant products."[461]

A final source of sensitive information at USDA is the Food Safety and Inspection Service's vulnerability assessments.[462] Among other things, these assessments "inform the development of countermeasures to help prevent or mitigate the impacts of an intentional attack on the food supply."[463]

2. FY 2018 Inspector General FISMA Report

The USDA IG contracted with RMA Associates ("RMA") to conduct an audit of its information security program. RMA rated the Department's information security at Level 2, "Defined" maturity level.[464] RMA added that in the absence of more widespread security policy implementation, the Department would be unable to accurately assess whether its controls "are operating as intended and are producing the desired outcome."[465]

Lack of Valid Authorities to Operate. While RMA noted that USDA has significantly decreased the number of systems operating without a valid authorization to operate, it still found 16 operational systems that lacked valid authorizations.[466] The Department informed the Subcommittee that it made over a 20 percent improvement in the number of systems with valid authorities over the last year and a half and now only have 11 systems lacking ATOs.[467] Specifically, "96 percent of USDA systems have valid Authority to Operate as opposed to 74 percent in FY17."[468] According to the IG, USDA must maintain that low level of expired authorizations to operate in order "to demonstrate achievement of a Managed and Measurable" maturity level.[469]

Use of Unsupported Systems. RMA found that unsupported software applications "exposed the Department to vulnerabilities that are difficult to effectively mitigate."[470] Use of unsupported software increases the likelihood that

---

[461] *Id.* at 9.
[462] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 18-155, BIODEFENSE: FEDERAL EFFORTS TO DEVELOP BIOLOGICAL THREAT AWARENESS, 46 (OCT. 2017).
[463] *Id.*
[464] Office of Inspector General, U.S. Dep't of Agriculture, 50501-0018-12, Fiscal Year 2018 Federal Information Security Modernization Act, 6 (Oct. 12, 2018).
[465] *Id.* at 7.
[466] *Id.* at 9.
[467] Email from U.S. Dep't of Agriculture to Subcommittee staff (June 7, 2019) (On file with Subcommittee).
[468] *Id.*
[469] Office of Inspector General, U.S. Dep't of Agriculture, 50501-0018-12, Fiscal Year 2018 Federal Information Security Modernization Act, 27 (Oct. 12, 2018).
[470] *Id.* at 11.

known cybersecurity vulnerabilities will be exploited.[471] RMA determined that "no waivers were provided for the unsupported software."[472]

Failure to Remediate Vulnerabilities. RMA specifically noted USDA's failure to remediate known vulnerabilities in a timely fashion.[473] At one USDA sub-agency, 49 percent of critical and high vulnerabilities were outstanding for 2 to 5 years, and an additional 12 percent for over 5 years.[474] The general department policy requires that high risk vulnerabilities be remediated within 30 days or that a Plan of Action and Milestones be established if it is determined that the 30 day window is not feasible.[475]

In a similar finding, RMA determined that USDA is not applying software patches and upgrades in a timely fashion.[476] This failure "increases the risk that known vulnerabilities will be exploited."[477] Moreover, USDA currently operates software that is no longer supported by the vendor, which exposes "the Department to vulnerabilities that are difficult to effectively mitigate."[478] This is a particular issue at USDA because the Department has many customized systems for which the vendor does not release periodic patches.[479]

Failure to Provide for the Adequate Protection of PII. RMA determined that USDA has yet to finalize a data protection and privacy policy to protect PII.[480] Without a final policy, the "decentralized governance of PII throughout the Department" will continue.[481] This decentralization is problematic because of the PII maintained by the Department. The Department informed the Subcommittee that since RMA's audit, it has implemented Microsoft Data Loss Prevention technology that "notifies employees when they are sending PII outside of USDA."[482]

Additional Cybersecurity Issues at USDA. RMA furthermore determined that USDA failed to ensure that all contingency plans were appropriately tested and reviewed to best "strengthen the effectiveness of each contingency plan."[483] Without proper testing, USDA runs the risk that each contingency plan will not work

---

[471] *Id.*
[472] *Id.*
[473] *Id.* at 10.
[474] *Id.*
[475] *Id.*
[476] *Id.* at 11.
[477] *Id.*
[478] *Id.*
[479] Briefing with the U.S. Dep't of Agriculture, Office of Inspector General (Nov. 20, 2018).
[480] Office of Inspector General, U.S. Dep't of Agriculture, 50501-0018-12, Fiscal Year 2018 Federal Information Security Modernization Act, 12 (Oct. 12, 2018).
[481] *Id.* at 13.
[482] Email from U.S. Dep't of Agriculture to Subcommittee staff (June 7, 2019) (On file with Subcommittee).
[483] Office of Inspector General, U.S. Dep't of Agriculture, 50501-0018-12, Fiscal Year 2018 Federal Information Security Modernization Act, 14 (Oct. 12, 2018).

properly in event of an actual breach.[484] The more a plan is tested, the more efficient it will be in real time and the better IT staff will be able to protect sensitive information.[485]

3. Persistent Problems Based on Prior IG FISMA Audits

Lack of Valid Authorities to Operate. In *every* year since FY 2009, the IG found that USDA maintained systems without a valid authority to operate.[486] This issue reached its peak at USDA in FY 2017 when auditors found 90 systems with invalid authorizations.[487] Although the number of systems with invalid authorizations has dropped to 11, this issue has been highlighted by the IG for a decade.[488] As a result, USDA is "vulnerable because the systems have not been through proper security testing."[489]

Use of Unsupported Systems. The IG determined that USDA used unsupported systems in 2009, 2014, 2015, 2016, and 2018.[490] For example, in 2015, the IG found that USDA employed a total of 240 machines using operating systems

---

[484] Briefing with the U.S. Dep't of Agriculture, Office of Inspector General (Nov. 20, 2018).
[485] *Id.*
[486] Office of Inspector General, U.S. Dep't of Agriculture, 50501-15-FM, Fiscal Year 2009 Federal Information Security Management Act, 4 (Nov. 2009); Office of Inspector General, U.S. Dep't of Agriculture, 50501-02-IT, Fiscal Year 2010 Federal Information Security Management Act, 18 (Nov. 2010); Office of Inspector General, U.S. Dep't of Agriculture, 50501-0002-12, Fiscal Year 2011 Federal Information Security Management Act, 61 (Nov. 2011); Office of Inspector General, U.S. Dep't of Agriculture, 50501-0003-12, Fiscal Year 2012 Federal Information Security Management Act, 6 (Nov. 2012); Office of Inspector General, U.S. Dep't of Agriculture, 50501-0004-12, Fiscal Year 2013 Federal Information Security Management Act, 30 (Nov. 2013); Office of Inspector General, U.S. Dep't of Agriculture, 50501-0006-12, Fiscal Year 2014 Federal Information Security Management Act, 4 (Nov. 2014); Office of Inspector General, U.S. Dep't of Agriculture, 50501-0018-12, Fiscal Year 2015 Federal Information Security Modernization Act, 6 (Nov. 10, 2015); Office of Inspector General, U.S. Dep't of Agriculture, 50501-0012-12, Fiscal Year 2016 Federal Information Security Modernization Act, 6 (Nov. 2016); Office of Inspector General, U.S. Dep't of Agriculture, 50501-0015-12, Fiscal Year 2017 Federal Information Security Modernization Act, 7 (Oct. 2017); Office of Inspector General, U.S. Dep't of Agriculture, 50501-0018-12, Fiscal Year 2018 Federal Information Security Modernization Act, 9 (Oct. 12, 2018).
[487] Office of Inspector General, U.S. Dep't of Agriculture, 50501-0015-12, Fiscal Year 2017 Federal Information Security Modernization Act, 7 (Oct. 2017).
[488] Email from U.S. Dep't of Agriculture to Subcommittee staff (June 7, 2019) (On file with Subcommittee).
[489] Office of Inspector General, U.S. Dep't of Agriculture, 50501-0008-12, Fiscal Year 2015 Federal Information Security Modernization Act, 6 (Nov. 10, 2015).
[490] Office of Inspector General, U.S. Dep't of Agriculture, 50501-15-FM, Fiscal Year 2009 Federal Information Security Management Act, 4 (Nov. 2009); Office of Inspector General, U.S. Dep't of Agriculture, 50501-0006-12, Fiscal Year 2014 Federal Information Security Management Act, 18 (Nov. 2014); Office of Inspector General, U.S. Dep't of Agriculture, 50501-0008-12, Fiscal Year 2015 Federal Information Security Modernization Act, 16 (Nov. 10, 2015); Office of Inspector General, U.S. Dep't of Agriculture, 50501-0012-12, Fiscal Year 2016 Federal Information Security Modernization Act, 24 (Nov. 2016); Office of Inspector General, U.S. Dep't of Agriculture, 50501-0018-12, Fiscal Year 2018 Federal Information Security Modernization Act, 11 (Oct. 12, 2018).

that were past end-of-support.[491] USDA has decreased the number of unsupported systems it uses in recent years, but has not completely eliminated them.[492] The continued use of these systems exposes the Department to greater risk of malware and increased risk of unauthorized access.[493]

Failure to Remediate Vulnerabilities. With the exception of 2011 and 2017, the IG found that USDA failed to properly apply security patches in *every* fiscal year since 2008.[494] In FY 2014, the IG determined that one USDA sub-agency failed to apply 82.5 percent of patches that were available from the vendor.[495] In FY 2016, the IG again evaluated a USDA sub-agency and found that over 13 percent of vulnerabilities were not remediated with an available vendor patch within 90 days.[496] It is important that USDA continue to improve in this area because "patching or upgrading is usually the most effective way to mitigate security flaws in software and is often the only fully effective solution."[497]

Failure to Compile an Accurate and Comprehensive IT Asset Inventory. In *seven* consecutive fiscal years spanning from 2010 to 2016, the IG determined that USDA failed to compile an accurate IT asset inventory.[498] One specific issue that

---

[491] Office of Inspector General, U.S. Dep't of Agriculture, 50501-0008-12, Fiscal Year 2015 Federal Information Security Modernization Act, 16 (Nov. 10, 2015).
[492] Office of Inspector General, U.S. Dep't of Agriculture, 50501-0012-12, Fiscal Year 2016 Federal Information Security Modernization Act, 24 (Nov. 2016); Office of Inspector General, U.S. Dep't of Agriculture, 50501-0018-12, Fiscal Year 2018 Federal Information Security Modernization Act, 11 (Oct. 12, 2018).
[493] Office of Inspector General, U.S. Dep't of Agriculture, 50501-0012-12, Fiscal Year 2016 Federal Information Security Modernization Act, 24 (Nov. 2016).
[494] Office of Inspector General, U.S. Dep't of Agriculture, 50501-13-FM, Fiscal Year 2008 Federal Information Security Management Act, vi (Sept. 2008); Office of Inspector General, U.S. Dep't of Agriculture, 50501-15-FM, Fiscal Year 2009 Federal Information Security Management Act, 8 (Nov. 2009); Office of Inspector General, U.S. Dep't of Agriculture, 50501-02-IT, Fiscal Year 2010 Federal Information Security Management Act, 4 (Nov. 2010); Office of Inspector General, U.S. Dep't of Agriculture, 50501-0003-12, Fiscal Year 2012 Federal Information Security Management Act, 20 (Nov. 2012); Office of Inspector General, U.S. Dep't of Agriculture, 50501-0004-12, Fiscal Year 2013 Federal Information Security Management Act, 20 (Nov. 2013); Office of Inspector General, U.S. Dep't of Agriculture, 50501-0006-12, Fiscal Year 2014 Federal Information Security Management Act, 16 (Nov. 2014); Office of Inspector General, U.S. Dep't of Agriculture, 50501-0008-12, Fiscal Year 2015 Federal Information Security Modernization Act, 16 (Nov. 10, 2015); Office of Inspector General, U.S. Dep't of Agriculture, 50501-0012-12, Fiscal Year 2016 Federal Information Security Modernization Act, 24 (Nov. 2016); Office of Inspector General, U.S. Dep't of Agriculture, 50501-0018-12, Fiscal Year 2018 Federal Information Security Modernization Act, 6, 14 (Oct. 12, 2018).
[495] Office of Inspector General, U.S. Dep't of Agriculture, 50501-0006-12, Fiscal Year 2014 Federal Information Security Modernization Act, 16 (Nov. 2014).
[496] Office of Inspector General, U.S. Dep't of Agriculture, 50501-0012-12, Fiscal Year 2016 Federal Information Security Modernization Act, 24 (Nov. 2016).
[497] Office of Inspector General, U.S. Dep't of Agriculture, 50501-0018-12, Fiscal Year 2018 Federal Information Security Modernization Act, 11 (Oct. 12, 2018).
[498] Office of Inspector General, U.S. Dep't of Agriculture, 50501-02-IT, Fiscal Year 2010 Federal Information Security Management Act, 6, 19 (Nov. 2010); Office of Inspector General, U.S. Dep't of Agriculture, 50501-0002-12, Fiscal Year 2011 Federal Information Security Management Act, 51 (Nov. 2011); Office of Inspector General, U.S. Dep't of Agriculture, 50501-0003-12, Fiscal Year 2012

the IG highlighted was USDA's failure to inventory systems used by contractors.[499] The Department recently took steps to address this longstanding issue by introducing enterprise-wide tools to inventory and track IT assets.[500]

Failure to Provide for the Adequate Protection of PII. Annual FISMA audits in 2008 and 2018 revealed that USDA had weaknesses in its protection of PII.[501] The Department continues to struggle to define policies and procedures that protect PII and has "led to a decentralized governance of PII throughout the Department."[502] This decentralization is a contributing factor in the Department's lack of a "finalized, overarching data protection and privacy policy."[503]

4. CIO Turnover and OCIO Challenges

From 2012 to 2017, USDA had six different CIOs.[504] The current CIO has been in office for roughly one year and four months after assuming the post in February 2018.[505]

A 2018 GAO report found that USDA did not at all define the CIO's role with respect to IT strategic planning.[506] Moreover, USDA's policies only partially addressed the CIO's role in IT workforce management, failing to completely detail how the CIO is to review the skills and deficiencies of USDA's IT personnel and where improvements can be made.[507] Since the release of that GAO report, USDA

Federal Information Security Management Act, 44-45 (Nov. 2012); Office of Inspector General, U.S. Dep't of Agriculture, 50501-0004-12, Fiscal Year 2013 Federal Information Security Management Act, 8, 28 (Nov. 2013); Office of Inspector General, U.S. Dep't of Agriculture, 50501-0006-12, Fiscal Year 2014 Federal Information Security Management Act, 6 (Nov. 2014); Office of Inspector General, U.S. Dep't of Agriculture, 50501-0008-12, Fiscal Year 2015 Federal Information Security Modernization Act, 8, 22 (Nov. 10, 2015); Office of Inspector General, U.S. Dep't of Agriculture, 50501-0012-12, Fiscal Year 2016 Federal Information Security Modernization Act, 7, 15 (Nov. 2016).

[499] Office of Inspector General, U.S. Dept. of Agriculture, 50501-0012-12, Fiscal Year 2016 Federal Information Security Modernization Act, 7 (Nov. 2016).

[500] Office of Inspector General, U.S. Dep't of Agriculture, 50501-0018-12, Fiscal Year 2018 Federal Information Security Modernization Act, 9 (Oct. 12, 2018).

[501] Office of Inspector General, U.S. Dep't of Agriculture, 50501-13-FM, Fiscal Year 2008 Federal Information Security Management Act, iii (Sept. 2008); Office of Inspector General, U.S. Dep't of Agriculture, 50501-0018-12, Fiscal Year 2018 Federal Information Security Modernization Act, 12 (Oct. 12, 2018).

[502] Office of Inspector General, U.S. Dep't of Agriculture, 50501-0018-12, Fiscal Year 2018 Federal Information Security Modernization Act, 12–13 (Oct. 12, 2018).

[503] *Id.* at 12.

[504] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 18-93, FEDERAL INFORMATION OFFICERS: CRITICAL ACTIONS NEEDED TO ADDRESS SHORTCOMINGS AND CHALLENGES IN IMPLEMENTING RESPONSIBILITIES, 68 (AUG. 2018).

[505] *Chief Information Officer*, U.S. Dep't of Agriculture, https://www.ocio.usda.gov/leaders/gary-washington.

[506] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 18-93, FEDERAL INFORMATION OFFICERS: CRITICAL ACTIONS NEEDED TO ADDRESS SHORTCOMINGS AND CHALLENGES IN IMPLEMENTING RESPONSIBILITIES, 68 (AUG. 2018).

[507] *Id.*

has issued an agency directive that better defines the CIO's role with respect to human resources, acquisition, and IT strategic planning.[508]

5. IT Spending on Operations and Maintenance

Of the agencies examined in this report, USDA has the second highest budget request for O&M as a percentage of its overall IT budget.[509] In total, USDA requested roughly $2.5 billion for O&M—roughly 86 percent of the overall IT budget request.[510] USDA told the Subcommittee it now only spends $3.75 million on the maintenance of legacy systems.[511]

One example of a legacy system that illustrates USDA's heavy O&M spending is its Resource Ordering and Status System ("ROSS"). USDA launched ROSS in 1998 making it approximately 21 years old.[512] At USDA, ROSS is "used to mobilize and deploy a multitude of resources, including qualified individuals, teams, aircraft, equipment, and supplies to fight wildland fires and respond to all hazard incidents."[513] Despite the importance of this system, the U.S. Forest Service warns "the technology used by ROSS is on the verge of technical obsolescence."[514] Although ROSS was supposed to be retired in 2018, that did not occur.[515] USDA is currently in the process of developing ROSS's replacement with an estimated completion date of September 2019.[516] That replacement system is scheduled to go live in January 2020.[517]

---

[508] Email from U.S. Dep't of Agriculture to Subcommittee staff (June 7, 2019) (On file with Subcommittee).
[509] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 18-93, FEDERAL INFORMATION OFFICERS: CRITICAL ACTIONS NEEDED TO ADDRESS SHORTCOMINGS AND CHALLENGES IN IMPLEMENTING RESPONSIBILITIES, 68 (AUG. 2018).
[510] *Id.*
[511] Email from U.S. Dep't of Agriculture to Subcommittee staff (May 20, 2019) (On file with Subcommittee).
[512] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 16-468, INFORMATION TECHNOLOGY: FEDERAL AGENCIES NEED TO ADDRESS AGING LEGACY SYSTEMS, 58 (MAY 2016).
[513] *Id.*
[514] *Id.*
[515] Email from U.S. Dep't of Agriculture to Subcommittee staff (April 11, 2019) (On file with Subcommittee).
[516] *Id.*
[517] *Id.*

F. The Department of Health and Human Services

The Department of Health and Human Service's ("HHS") mission is "to enhance and protect the health and well-being of all Americans."[518] HHS seeks to execute that mission "by providing for effective health and human services and fostering advances in medicine, public health, and social services."[519]

Recent events have highlighted HHS's struggle to institute adequate security controls, particularly regarding the protection of PII. In October of 2018, a breach of Healthcare.gov compromised the confidential records of roughly 75,000 consumers.[520]

1. Examples of Information Held by the Department of Health and Human Services

HHS holds PII such as Social Security numbers, names, addresses, and employee records.[521] HHS operating divisions maintain their own sensitive information stockpiles. For example, the Food and Drug Administration ("FDA") has potentially market sensitive information pertaining to pharmaceuticals and medical devices.[522] Moreover, the National Institute of Health ("NIH") houses sensitive information including patient records.[523]

An example of an HHS database that maintains large quantities of PII is the Centers for Medicare and Medicaid Services ("CMS") Marketplace Consumer Record ("MCR") system. This system "makes available the complete enrollment and eligibility data to respond to consumer inquiries."[524] MCR maintains data such as names, dates of birth, addresses, household income, employment information, Social Security numbers, and health insurance plan information.[525] This information allows other CMS programs resolve enrollment discrepancies and otherwise answer consumer questions related to their healthcare coverage.[526]

---

[518] *About HHS*, U.S. Dep't of Health & Human Services, https://www.hhs.gov/about/index.html.
[519] *Id.*
[520] Amy Goldstein, *Consumer data compromised in Affordable Care Act enrollment portal*, WASH. POST, Oct. 19, 2018, https://www.washingtonpost.com/national/health-science/consumer-data-compromised-in-affordable-care-act-enrollment-portal/2018/10/19/af39c822-d3e6-11e8-83d6-291fcead2ab1_story.html?utm_term=.6f00c06a4d08; Stephanie Armour, *Hackers Breach Healthcare.gov*, WALL ST. J., Oct. 19, 2018, https://www.wsj.com/articles/hackers-breach-healthcare-gov-1539991262.
[521] Briefing with the U.S. Dep't of Health and Human Services, Office of Inspector General (Nov. 8, 2018).
[522] *Id.*
[523] *Id.*
[524] U.S. Dep't of Health & Human Services, Privacy Impact Assessment Marketplace Consumer Record, (Nov. 11, 2016).
[525] *Id.*
[526] *Id.*

Another notable PII database is the National Institute of Health's ("NIH") Clinical Research Information System ("CRIS"). Generally speaking, CRIS "supports clinical care, collects data for research, and supports hospital operations."[527] Patient information collected as part of this effort includes names, Social Security numbers, medical notes, height, weight, medications administered and services provided.[528] Access to this patient information of this kind assists providers in making "appropriate clinical care and research decisions."[529]

Similar to USDA, HHS also has a counterterrorism role that requires it to aggregate sensitive information to protect "the United States from chemical, biological, radiological, nuclear, and emerging infectious disease threats."[530] Specifically, FDA develops medical countermeasures "that may be used in the event of a potential public health emergency stemming from a terrorist attack with a biological, chemical, or radiological/nuclear material, or a naturally occurring emerging disease."[531] HHS's Centers for Disease Control and Prevention ("CDC") also supports this broader department mission through its maintenance of the Strategic National Stockpile.[532] The Strategic National Stockpile "is the nation's largest supply of potentially life-saving pharmaceuticals and medical supplies."[533] The medical countermeasures stored in this stockpile include countermeasures not available on the market.[534]

2. FY 2018 Inspector General FISMA Report

The HHS IG contracted with Ernst and Young ("EY") to conduct its annual review of FISMA compliance. EY assigned a maturity level rating of 2, "Defined," for three of the five function areas.[535] This rating falls well below the level 4 rating, "Managed and Measureable," needed for HHS to have an effective information security program.

---

[527] U.S. Dep't of Health & Human Services, Privacy Impact Clinical Research Information System, (Sept. 29, 2016).
[528] *Id.*
[529] *Id.*
[530] *Counterterrorism and Emerging Threats*, U.S. Dep't of Health & Human Services, Food & Drug Admin., https://www.fda.gov/emergency-preparedness-and-response/counterterrorism-and-emerging-threats.
[531] *What are Medical Countermeasures?*, U.S. Dep't of Health & Human Services, Food & Drug Admin., https://www.fda.gov/emergency-preparedness-and-response/about-mcmi/what-are-medical-countermeasures.
[532] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-18-155, BIODEFENSE: FEDERAL EFFORTS TO DEVELOP BIOLOGICAL THREAT AWARENESS, 11 (OCT. 2017).
[533] *Id.* at n.26.
[534] *Id.*
[535] Office of Inspector General, U.S. Dep't of Health & Human Services, A-18-18-11200, Review of the Department of Health and Human Services' Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2018, 4 (Apr. 2019).

Lack of Valid Authorities to Operate. EY identified weaknesses in HHS's information security continuous monitoring function.[536] In particular, EY discovered several systems that were "operating with an expired Authorization to Operate."[537] As a result of these weaknesses, HHS does not have "a complete list of required processes to protect their information assets."[538] Without this list, HHS may not detect potential high-risk threats that could lead to "unauthorized access or changes to information systems, and misuse, compromise, or loss of confidential data and resources."[539]

Use of Unsupported Systems. EY also found HHS weaknesses in configuration management.[540] Configuration management refers to "activities that pertain to the operations, administration, maintenance, and configuration of networked systems and their security posture."[541] A specific identified weakness in this area was EY's finding that HHS "had numerous IT assets deployed with security configurations that were no longer being supported by the vendor to address emerging cyber threats."[542]

HHS's Medicare Enrollment system is an example of a legacy system.[543] In light of the antiquated nature of system, HHS now has a difficult time finding people who know how to work with this system.[544]

Failure to Compile an Accurate and Comprehensive IT Asset Inventory. HHS has not implemented an effective process for developing and maintaining an inventory of all software assets on its network.[545] Although HHS has instituted a process for compiling an IT asset inventory, the Department failed to ensure that some hardware assets "connected to the network are subject to the monitoring processes defined within the organization's information security continuous monitoring strategy."[546] Without an accurate inventory that lists all systems that are operational across the Department, HHS will be unable to secure its network.[547]

Failure to Provide for the Adequate Protection of PII. Recent events have demonstrated HHS's struggle to ensure that adequate security controls are

---

[536] *Id.* at 12.
[537] *Id.*
[538] *Id.*
[539] *Id.*
[540] *Id.* at 7.
[541] *Id.*
[542] *Id.*
[543] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 16-468, INFORMATION TECHNOLOGY: FEDERAL AGENCIES NEED TO ADDRESS AGING LEGACY SYSTEMS, 46 (MAY 2016).
[544] Briefing with the U.S. Dep't of Health and Human Services, Office of the Inspector General (Nov. 8, 2018).
[545] Office of Inspector General, U.S. Dep't of Health & Human Services, Inspector General Section Report: 2018 Annual FISMA Report, app. C at 1 (April 2019).
[546] *Id.*
[547] Briefing with the U.S. Dep't of Health and Human Services, Office of the Inspector General (Nov. 8, 2018).

instituted across HHS divisions and offices.[548] In October 2018, a breach of Healthcare.gov compromised the confidential records of roughly 75,000 consumers.[549] The breach itself involved a system "used by agents and brokers as part of the insurance program," and exposed PII such as credit information.[550] HHS officials had been on notice of Healthcare.gov's cybersecurity weaknesses as far back as 2015, when the IG issued a report saying the "sensitive data on millions of consumers was being stored in a system with fundamental security risks."[551]

3. Persistent Problems Based on Prior IG FISMA Audits

Lack of Valid Authorities to Operate. In *nine* consecutive fiscal years, from FY 2009 to FY 2018, auditors determined that HHS operated systems without valid authorities to operate.[552] In FY 2012 for example, auditors determined that NIH

---

[548] *Id.*

[549] Amy Goldstein, *Consumer data compromised in Affordable Care Act enrollment portal*, WASH. POST, Oct. 19, 2018, https://www.washingtonpost.com/national/health-science/consumer-data-compromised-in-affordable-care-act-enrollment-portal/2018/10/19/af39c822-d3e6-11e8-83d6-291fcead2ab1_story.html?utm_term=.6f00c06a4d08; Stephanie Armour, *Hackers Breach Healthcare.gov*, WALL ST. J., Oct. 19, 2018, https://www.wsj.com/articles/hackers-breach-healthcare-gov-1539991262.

[550] Amy Goldstein, *Consumer data compromised in Affordable Care Act enrollment portal*, WASH. POST, Oct. 19, 2018, https://www.washingtonpost.com/national/health-science/consumer-data-compromised-in-affordable-care-act-enrollment-portal/2018/10/19/af39c822-d3e6-11e8-83d6-291fcead2ab1_story.html?utm_term=.6f00c06a4d08.

[551] Stephanie Armour, *Hackers Breach Healthcare.gov*, WALL ST. J., Oct. 19, 2018, https://www.wsj.com/articles/hackers-breach-healthcare-gov-1539991262.

[552] Office of Inspector General, U.S. Dep't of Health & Human Services, A-18-09-30210, Review of the Office of the Secretary's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2009, 25 (Nov. 2009); Office of Inspector General, U.S. Dep't of Health & Human Services, A-18-10-30240, Review of the Office of the Centers for Medicare & Medicaid Services' Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2010, 17 (Dec. 2010); Office of Inspector General, U.S. Dep't of Health & Human Services, A-18-11-30260, Review of the National Institutes of Health's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2011, iii (Jan. 2012); Office of Inspector General, U.S. Dep't of Health & Human Services, A-18-12-30080, Review of the National Institutes of Health's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2012, 6 (Jan. 2013); Office of Inspector General, U.S. Dep't of Health & Human Services, A-18-13-30440, Review of the Food and Drug Administration's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2013, 14, 38 (Feb. 2014); Office of Inspector General, U.S. Dep't of Health & Human Services, A-18-114-30320, Review of the Office of the Secretary's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2014, 61 (Dec. 2014); Office of Inspector General, U.S. Dep't of Health & Human Services, 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, 21 (Mar. 2016); Office of Inspector General, U.S. Dep't of Health & Human Services, 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, 8 (Feb. 2017); Office of Inspector General, U.S. Dep't of Health & Human Services, A-18-18-11200, Review of the Department of Health and Human Services' Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2018, 12 (Apr. 2019).

and CMS had 11 and 25 expired authorizations respectively.[553] In FY 2015, of the five HHS subdivisions evaluated by auditors, three were operating systems lacking valid authorizations.[554] According to the IG, without a more consistent security authorization process, "HHS management will not be able to evaluate and determine whether appropriate security measures are in place for its IT systems and operations."[555]

Use of Unsupported Systems. Since FY 2008, auditors noted HHS use of unsupported systems *nine* times.[556] For instance, in FY 2014, auditors found that the FDA was still using a version of Microsoft Windows 2000 Server even though that system had been unsupported since 2010.[557] In that same fiscal year, auditors also found that seven servers in the Office of the Secretary were using Windows

---

[553] Office of Inspector General, U.S. Dep't of Health & Human Services, A-18-12-30080, Review of the National Institutes Health's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2012, 6 (Jan. 2013); Office of Inspector General, U.S. Dep't of Health & Human Services, A-18-12-30310, Review of the Centers for Medicare and Medicaid Services' Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2012, 15 (Jan. 2013).
[554] Office of Inspector General, U.S. Dep't of Health & Human Services, 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, 21 (March 2016).
[555] Office of Inspector General, U.S. Dep't of Health & Human Services, 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, 8 (Feb. 2017).
[556] Office of Inspector General, U.S. Dep't of Health & Human Services, A-18-08-30160, Audit of the Food and Drug Administration's Security Program, 12,16 (Oct. 2008); Office of Inspector General, U.S. Dep't of Health & Human Services, A-18-09-30110, Review of the Centers for Medicare & Medicaid Services' Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2009, 11 (Nov. 2009); Office of Inspector General, U.S. Dep't of Health & Human Services, Submission for Fiscal Year 2010 Federal Information Security Management Act Executive Summary and OPDIV Reports, 6 (Dec. 2010); Office of Inspector General, U.S. Dep't of Health & Human Services, A-18-11-30320, Review of the Office of the Secretary's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2011, 10 (Jan. 2012); Office of Inspector General, U.S. Dep't of Health & Human Services, A-18-12-30440, Review of the Food and Drug Administration's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2012, 8 (Jan. 2013); Office of Inspector General, U.S. Dep't of Health & Human Services, A-18-13-30440, Review of the Food and Drug Administration's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2013, 7–8 (Feb. 2014); Office of Inspector General, U.S. Dep't of Health & Human Services, A-18-14-30440, Review of the Food and Drug Administration's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2014, 10 (Jan. 2015); Office of Inspector General, U.S. Dep't of Health & Human Services, A-18-17-11200, Review of the Department of Health and Human Services' Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2017, 6 (Mar. 2018); Office of Inspector General, U.S. Dep't of Health & Human Services, A-18-18-11200, Review of the Department of Health and Human Services' Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2018, 7 (Apr. 2019).
[557] Office of Inspector General, U.S. Dep't of Health & Human Services, A-18-14-30440, Review of the Food and Drug Administration's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2014, 10 (Jan. 2015).

Server 2000.[558] Lastly, in FY 2014, the Indian Health Service ("IHS") alone was operating Windows 2000 on 58 servers.[559] These long-standing security deficiencies could potentially "leave HHS data susceptible to unauthorized disclosure, modification, or non-availability of data."[560]

Failure to Remediate Vulnerabilities. The IG found HHS failed to appropriately apply security patches and remediate vulnerabilities *eight* times over the past eleven fiscal years.[561] In FY 2013, when assessing the cybersecurity protocols of an HHS operating division that supports important healthcare functions, auditors determined that several high severity patches were missing on operating division servers.[562] The IG also found hundreds of patches were missing on one or more servers for that same HHS operating division.[563]

Failure to Compile an Accurate & Comprehensive IT Asset Inventory. Since FY 2008, the IG noted HHS's lack of a comprehensive IT asset inventory *nine* times.[564] During this time, HHS has struggled to reconcile sub-agency inventories

---

[558] Office of Inspector General, U.S. Dep't of Health & Human Services, A-18-14-30320, Review of the Office of the Secretary's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2014, 7 (Dec. 2014).
[559] Office of Inspector General, U.S. Dep't of Health & Human Services, A-18-14-30260, Review of the Indian Health Service's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2014, 8 (Jan. 2015).
[560] Office of Inspector General, U.S. Dep't of Health & Human Services, A-18-17-11200, Review of the Department of Health and Human Services' Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2017, 6 (Mar. 2018).
[561] Office of Inspector General, U.S. Dep't of Health & Human Services, A-04-08-05068, Audit of the Centers for Disease Control and Prevention's Compliance with the Federal Information Security Management Act for Fiscal Year 2008, 5,7 (Oct. 2008); Office of Inspector General, U.S. Dep't of Health & Human Services, A-04-09-05001, Review of the Centers for Disease Control and Prevention's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2009, 6 (Nov. 2009); Office of Inspector General, U.S. Dep't of Health & Human Services, Submission for Fiscal Year 2010 Federal Information Security Management Act Executive Summary and OPDIV Reports, 6 (Dec. 2010); Office of Inspector General, U.S. Dep't of Health & Human Services, A-04-12-05041, Centers for Disease Control and Prevention, Federal Information Security Management Act Program Audit for Fiscal Year 2012, 10 (Jan. 2013); Office of Inspector General, U.S. Dep't of Health & Human Services, A-18-13-30080, Review of the National Institutes of Health's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2013, 7 (Feb. 2014); Office of Inspector General, U.S. Dep't of Health & Human Services, A-18-14-30270, Review of the Office of the National Institute of Health's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2014, 8 (Dec. 2014); Office of Inspector General, U.S. Dep't of Health & Human Services, 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 (Mar. 2016); Office of Inspector General, U.S. Dep't of Health & Human Services, 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 (Feb. 2017).
[562] Email from U.S. Dep't of Health & Human Services to Subcommittee staff (June 19, 2019) (On file with Subcommittee).
[563] *Id.*
[564] Office of Inspector General, U.S. Dep't of Health & Human Services, A-18-08-30140, Audit of the Department's Security Program, 5 (Sept. 2008); Office of Inspector General, U.S. Dep't of Health &

with the one maintained at the department level.[565] The lack of a comprehensive IT asset inventory can "lead to inadequate controls across systems that could compromise the security of the systems and lead to unauthorized access and manipulation of data."[566]

4. CIO Turnover and OCIO Challenges

HHS experienced less CIO turnover relative to other federal agencies with a total of three CIOs from 2012 to 2017.[567] HHS just named a new CIO in May 2019.[568] The Department reassigned the previous CIO to the Office of the Surgeon General.[569] That reassignment followed a House Energy and Commerce Committee Investigation "to determine if HHS penalized two former Healthcare Cybersecurity Communications and Integration Center ("HCCIC") leaders for whistleblowing."[570]

Recently, GAO evaluated the extent to which HHS policies formally outline and document the responsibilities of its CIO. GAO determined that HHS policies failed to sufficiently address both how the CIO is to participate in IT Workforce

---

Human Services, Submission of Fiscal Year 2009 Federal Information Security Management Act, 8 (Nov. 2009); Office of Inspector General, U.S. Dep't of Health & Human Services, A-18-10-30270, Review of the Office of the Secretary's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2010, 12 (Dec. 2010); Office of Inspector General, U.S. Dep't of Health & Human Services, A-18-11-30320, Review of the Office of the Secretary's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2011, 6 (Jan. 2012); Office of Inspector General, U.S. Dep't of Health & Human Services, A-18-12-30080, Review of the National Institutes of Health's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2012, 27 (Jan. 2013); Office of Inspector General, U.S. Dep't of Health & Human Services, A-18-13-00040, Review of the Indian Health Services' Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2013, 4 (Feb. 2014); Office of Inspector General, U.S. Dep't of Health & Human Services, A-18-14-30440, Review of the Food and Drug Administration's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2014, 46 (Dec. 2014); Office of Inspector General, U.S. Dep't of Health & Human Services, 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, 8,15,20 (Mar. 2016); Office of Inspector General, U.S. Dep't of Health & Human Services, Inspector General Section Report: 2018 Annual FISMA Report, app. C at 1 (Apr. 2019).

[565] Office of Inspector General, U.S. Dep't of Health & Human Services, 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, 8 (Mar. 2016).

[566] *Id.*

[567] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 18-93, FEDERAL INFORMATION OFFICERS: CRITICAL ACTIONS NEEDED TO ADDRESS SHORTCOMINGS AND CHALLENGES IN IMPLEMENTING RESPONSIBILITIES, 78 (AUG. 2018).

[568] Jason Miller, *Why the new HHS CIO is not your usual suspect*, FED. NEWS NETWORK, May 24, 2019, https://federalnewsnetwork.com/cio-news/2019/05/why-the-new-hhs-cio-is-not-your-usual-suspect/.

[569] Jessica Davis, *HHS reassigns CIO Beth Killoran in latest staffing shake-up*, HEALTHCARE IT NEWS, Aug. 21, 2018, https://www.healthcareitnews.com/news/hhs-reassigns-cio-beth-killoran-latest-staffing-shake.

[570] *Id.*

assessment and IT strategic planning.[571] With respect to IT strategic planning, HHS policies did not address the CIO's role in evaluating how well IT supports agency programs or how the CIO is to participate in the consultation of agency processes before making significant IT investments.[572] For IT workforce assessment, Department policies did not address how the CIO is to "assess the extent to which agency personnel meet IT management knowledge and skill requirements" or develop strategies "to rectify any knowledge and skill deficiencies."[573]

5. IT Spending on Operations and Maintenance

In FY 2018, HHS requested $13.8 billion in total IT funding.[574] It specifically requested $10.2 billion for O&M—roughly 73 percent of HHS's overall IT budget request.[575] When asked how much O&M spending goes towards the maintenance of legacy systems, the Department told the Subcommittee that it does "not yet have an easily accessible and synthesized view of O&M costs spent on existing legacy technology."[576]

Although HHS cannot precisely quantify how much of O&M spending is devoted to the maintenance of legacy IT, the Department continues to operate these expensive systems. For example, HHS supports the Medicare Appeals System—which is nearly 14 years old.[577] This system serves as a case tracking system that facilitates the "maintenance and transfer of case specific data with regard to Medicare appeals through multiple levels of the appeal process."[578] As of 2016, and although the system is over ten years old, HHS officials said they have no current plans to address outdated gaps in the system saying, "that doing so is contingent on funding."[579] HHS recently informed the Subcommittee of a number of improvements it has made to the Medicare Appeals system including changes that improve provider experience and other services that improve "internal operational efficiencies" thereby streamlining the appeals process.[580] Nonetheless, these recent

---

[571] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 18-93, FEDERAL INFORMATION OFFICERS: CRITICAL ACTIONS NEEDED TO ADDRESS SHORTCOMINGS AND CHALLENGES IN IMPLEMENTING RESPONSIBILITIES, 78 (AUG. 2018).
[572] *Id.*
[573] *Id.*
[574] *Id.*
[575] *Id.*
[576] Email from U.S. Dep't of Health & Human Services to Subcommittee staff (May 23, 2019) (On file with Subcommittee).
[577] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 16-468, INFORMATION TECHNOLOGY: FEDERAL AGENCIES NEED TO ADDRESS AGING LEGACY SYSTEMS, 54 (MAY 2016).
[578] *Id.*
[579] *Id.*
[580] Email from U.S. Dep't of Health & Human Services to Subcommittee staff (May 1, 2019) (On file with Subcommittee).

improvements address the functionality of the system and do not specifically improve the system's security.[581]

G. The Department of Education

The Department of Education's mission is "to promote student achievement and preparation for global competitiveness by fostering educational excellence and ensuring equal access."[582] 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."[583]

1. Examples of Information Held by the Department of Education

One of Education's notable PII repositories is maintained by the Office of Federal Student Aid ("FSA"). FSA is responsible for determining which students attending postsecondary schools are eligible for federal financial assistance.[584] As part of that process, students and parents are required to submit the following information:

- **Student Demographics:** Name, address, Social Security number, telephone number, email address, marital status, and driver's license numbers.
- **Student Eligibility:** Citizenship status, dependency status, high school completion status, Selective Service System registration, and drug convictions.
- **Student Finances:** Tax-return filing status, adjusted gross income, cash, savings and checking account balances, untaxed income, and net worth.
- **Parent Demographics:** Name, Social Security number, email address, and marital status.
- **Parent Finances:** Tax return filing status, adjusted gross income, tax exemptions, and asset information.[585]

In FY 2018 alone, FSA processed more than 18.6 million Free Applications for Federal Student Aid ("FAFSA") and provided aid to more than 12.7 million students attending roughly 6,000 schools.[586]

---

[581] Telephone Call with U.S. Gov't Accountability Office Personnel (May 9, 2019).
[582] *Mission,* U.S. Dep't of Education, https://www2.ed.gov/about/overview/mission/mission.html.
[583] *Id.*
[584] 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 (NOV. 2017).
[585] *Id.* at 19.
[586] U.S. Dep't of Education, Federal Student Aid: Fiscal Year 2018 Annual Report, 8 (Nov. 15, 2018).

2. FY 2018 Inspector General FISMA Report

The Department of Education IG found that the Department's information security program was ineffective across all five NIST security functions.[587]

Use of Unsupported Systems. The IG discovered that the Department still relies on a number of applications and systems that vendors no longer support.[588] These systems are precarious from a security standpoint as they no longer receive the newest patches that update the security of applications or systems.[589] Therefore, the long-term use of these systems and applications could result in "data leakage and exposure of personally identifiable information that [could] . . . compromise the Department's integrity and reputation" as well as the reputations of the many Americans on which the Department has information.[590]

Failure to Remediate Vulnerabilities. The IG found that FSA "was not consistently applying software patches and security updates to its systems and information technology solutions."[591] As part of this failure, FSA failed to apply critical patch and security updates.[592] These patching weaknesses "could allow a malicious user to gain access to a system and user accounts, leading to identity theft or fraud."[593]

Failure to Provide for the Adequate Protection of PII. The latest FISMA audit documented that the Department of Education failed to adequately protect PII.[594] This task is especially difficult at Education because departmental access to PII is highly decentralized.[595] This decentralization is a result of the Department's reliance on contractors and college and university access to student financial aid information.[596] A 2017 GAO report also found several schools failed to identify risks to student information as required by Federal Trade Commission standards by neglecting to identify internal and external risks to student information and "design and implement safeguards to control risks identified in assessments."[597]

---

[587] Office of Inspector General, U.S. Dep't of Education, ED-OIG/A11S0001, The U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report For Fiscal Year 2018, 7 (Oct. 2018).
[588] *Id.* at 27.
[589] Briefing with the U.S. Dep't of Education, Office of Inspector General (Nov 5, 2018).
[590] Office of Inspector General, U.S. Dep't of Education, ED-OIG/A11S0001, The U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report For Fiscal Year 2018, 27–28 (Oct. 2018).
[591] *Id.* at 29.
[592] *Id.*
[593] *Id.*
[594] *Id.* at 28.
[595] Briefing with the U.S. Dep't of Education, Office of Inspector General (Nov 5, 2018).
[596] *Id.*
[597] 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, 49–50 (NOV. 2017).

The Education IG highlighted the exposure of Social Security information due to the Department's continued use of "Social Security numbers as an identifier" for user accounts on FSA websites.[598] The reliance on Social Security numbers in plain text is unsecure; any users with malware on their device "that captures screenshots could become a victim of identity theft."[599]

Decentralization also slows incident response time.[600] Under the Department's current configuration, contractors are required to report security incidents to the Department as they occur.[601] Because this reporting calls into question their own cybersecurity protocols, there are strong disincentives for contractors to report and, as the IG's audit found, it is not clear that security incidents are always reported in a timely fashion.[602]

Additional Cybersecurity Issues at Education. The IG determined that the Department failed to consistently ensure that agency websites were configured to use secure internet connections.[603] Out of 60 systems identified by the IG, only a third were "configured to use a trusted internet connection or managed trusted internet protocol services" as required by DHS and OMB.[604]

Similarly, the IG found that the Department was unable to prevent unauthorized devices from connecting to their network.[605] The IG first identified this problem in 2011, yet it remains unresolved.[606] Although the Department can now restrict non-government devices from initially connecting to its network, the IG found that non-government devices could still be reconnected for 90 second increments.[607] This narrow timeframe, according to the IG, is all a malicious actor needs to "launch an attack or gain intermittent access to internal network resources that could lead to data leakage or data exposure."[608]

---

[598] Office of Inspector General, U.S. Dep't of Education, ED-OIG/A11S0001, The U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report For Fiscal Year 2018, 28 (Oct. 2018).
[599] *Id.*
[600] Briefing with the U.S. Dep't of Education, Office of Inspector General (Nov 5, 2018).
[601] *Id.*
[602] *Id.*; Office of Inspector General, U.S. Dep't of Education, ED-OIG/A11S0001, The U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report For Fiscal Year 2018, 57 (Oct. 2018).
[603] Office of Inspector General, U.S. Dep't of Education, ED-OIG/A11S0001, The U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report For Fiscal Year 2018, 26 (Oct. 2018).
[604] *Id.*
[605] *Id.* at 34.
[606] *Id.*
[607] *Id.*
[608] *Id.*

3. Persistent Problems Based on Prior IG FISMA Audits

Lack of Valid Authorities to Operate. In *seven* fiscal years since 2008, the IG determined that Education maintained systems lacking valid authorities to operate.[609] In FY 2011, the IG found that out of the 100 systems listed on Education's inventory, 28 percent were operating on expired security authorizations.[610] This percentage remained relatively consistent over the next four fiscal years with the percentage of systems with expired authorizations fluctuating between 14 and 24 percent.[611] Because of these weaknesses in its security authorization process, Education "operated with unknown security risks for those systems with expired documentation."[612]

Use of Unsupported Systems. The IG determined that Education was using unsupported systems in FY 2015, 2017, and 2018.[613] For example in FY 2017, the

---

[609] Office of Inspector General, U.S. Dep't of Education, 2008 Annual FISMA Report, 6 (Oct. 1, 2008)(discussing that some Education departments "do not have current C&As for any of their systems"; According to best practices, an "ATO is dependent on a successful completion of the C&A process" Authorization to Operate, CDC Unified Process Practices Guide, https://www2.cdc.gov/cdcup/library/process_guides/doc/CDC_UP_Process_Guide_ato.doc); Office of Inspector General, U.S. Dep't of Education, 2009 Annual FISMA Report, 10−11 (Oct. 2009)(discussing that Authorizing Officials were "not presented with complete and reliable C&A information to facilitate an informed ATO decision"); Office of Inspector General, U.S. Dep't of Education, ED-OIG/A11L0003, The U.S. Department of Education's Federal Information Security Management Act of 2002 Report for Fiscal Year 2011, 9 (Oct. 2011); Office of Inspector General, U.S. Dep't of Education, ED-OIG/A11M0003, The U.S. Department of Education's Federal Information Security Management Act of 2002 Report for Fiscal Year 2012, 14 (Nov. 2012); Office of Inspector General, U.S. Dep't of Education, ED-OIG/A11N0001, The U.S. Department of Education's Federal Information Security Management Act of 2002 Report for Fiscal Year 2013, 19 (Nov. 2013); Office of Inspector General, U.S. Dep't of Education, ED-OIG/A11O0001, The U.S. Department of Education's Federal Information Security Management Act of 2002 Report for Fiscal Year 2014, 14 (Nov. 2014); Office of Inspector General, U.S. Dep't of Education, ED-OIG/A11P0001, The U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2015, 18 (Nov. 13, 2015).

[610] Office of Inspector General, U.S. Dep't of Education, ED-OIG/A11L0003, The U.S. Department of Education's Federal Information Security Management Act of 2002 Report for Fiscal Year 2011, 9 (Oct. 2011).

[611] Office of Inspector General, U.S. Dep't of Education, ED-OIG/A11M0003, The U.S. Department of Education's Federal Information Security Management Act of 2002 Report for Fiscal Year 2012, 14 (Nov. 2012); Office of Inspector General, U.S. Dep't of Education, ED-OIG/A11N0001, The U.S. Department of Education's Federal Information Security Management Act of 2002 Report for Fiscal Year 2013, 19 (Nov. 2013); Office of Inspector General, U.S. Dep't of Education, ED-OIG/A11O0001, The U.S. Department of Education's Federal Information Security Management Act of 2002 Report for Fiscal Year 2014, 15 (Nov. 2014); Office of Inspector General, U.S. Dep't of Education, ED-OIG/A11O0001, The U.S. Department of Education's Federal Information Security Management Act of 2002 Report for Fiscal Year 2015, 18 (Nov. 2015).

[612] Office of Inspector General, U.S. Dep't of Education, ED-OIG/A11O0001, The U.S. Department of Education's Federal Information Security Management Act of 2002 Report for Fiscal Year 2015, 19 (Nov. 2015).

[613] Office of Inspector General, U.S. Dep't of Education, ED-OIG/A11O0001, The U.S. Department of Education's Federal Information Security Management Act of 2002 Report for Fiscal Year 2015, 10

IG determined that both Education and FSA were using unsupported systems, and furthermore "unable to provide any documentation, such as Risk Assessment Forms, to justify the use of unsupported systems."[614] Because these systems no longer receive vendor patches, the Department's systems operate with "unknown risk and with no alternate plan of [action]."[615]

Failure to Remediate Vulnerabilities. The IG found that Education failed to adequately install security patches *eight* times since FY 2008.[616] Without an effective process that ensures the timely installation of patches, the Department is exposed "to unauthorized and unauthenticated access to the Department's network and data."[617] Moreover, the Department's "lack of suitable controls increases the potential of unauthorized changes to the operating system and application code, which could lead to the theft, destruction, or misuse of sensitive data."[618]

Failure to Compile an Accurate and Comprehensive IT Asset Inventory. The IG determined that Education maintained an incomplete IT Asset Inventory *four* times since FY 2008.[619] In FY 2017, the IG found that the Department failed to

---

(Nov. 2015); Office of Inspector General, U.S. Dep't of Education, ED-OIG/A11R0001, The U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2017, 20 (Oct. 2017); Office of Inspector General, U.S. Dep't of Education, ED-OIG/A11S0001, The U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2018, 27 (Oct. 31, 2018).

[614] Office of Inspector General, U.S. Dep't of Education, ED-OIG/A11R0001, The U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2017, 20 (Oct. 2017).

[615] *Id.*

[616] Office of Inspector General, U.S. Dep't of Education, 2008 Annual FISMA Report, 7 (Oct. 1, 2008); Office of Inspector General, U.S. Dep't of Education, 2010 Annual FISMA Report, 2–3 (Nov. 12, 2010); Office of Inspector General, U.S. Dep't of Education, ED-OIG/A11L0003, The U.S. Department of Education's Federal Information Security Management Act of 2002 Report for Fiscal Year 2011, 13–14 (Oct. 2011); Office of Inspector General, U.S. Dep't of Education, ED-OIG/A11M0003, The U.S. Department of Education's Federal Information Security Management Act of 2002 Report for Fiscal Year 2012, 8 (Nov. 2012); Office of Inspector General, U.S. Dep't of Education, ED-OIG/A11N0001, The U.S. Department of Education's Federal Information Security Management Act of 2002 Report for Fiscal Year 2013, 8–9 (Nov. 2013); Office of Inspector General, U.S. Dep't of Education, ED-OIG/A11O0001, The U.S. Department of Education's Federal Information Security Management Act of 2002 Report for Fiscal Year 2014, 7 (Nov. 2014); Office of Inspector General, U.S. Dep't of Education, ED-OIG/A11R0001, The U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2017, 22 (Oct. 2017); Office of Inspector General, U.S. Dep't of Education, ED-OIG/A11S0001, The U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2018, 29 (Oct. 31, 2018).

[617] Office of Inspector General, U.S. Dep't of Education, ED-OIG/A11N0001, The U.S. Department of Education's Federal Information Security Management Act of 2002 Report for Fiscal Year 2013, 9 (Nov. 2013).

[618] *Id.*

[619] Office of Inspector General, U.S. Dep't of Education, ED-OIG/A11M0003, The U.S. Department of Education's Federal Information Security Management Act of 2002 Report for Fiscal Year 2012, 19 (Nov. 2012); Office of Inspector General, U.S. Dep't of Education, ED-OIG/A11N0001, The U.S. Department of Education's Federal Information Security Management Act of 2002 Report for Fiscal Year 2013, 47 (Nov. 2013); Office of Inspector General, U.S. Dept. of Education, ED-OIG/A11O0001,

maintain an accurate inventory for all of its active websites.[620] In particular, the IG discovered 61 active websites that were not listed on the Department's inventory.[621] According to the IG, the failure to adequately track active websites "could lead to compromise and exposure of data without the Department knowing that it had occurred."[622]

Failure to Provide for the Adequate Protection of PII. The IG found Education did not adequately protect PII in *eight* annual FISMA audits since FY 2008.[623] One of the primary struggles that Education has in this area is using Social Security numbers as an identifier.[624] The Department asks users to provide their Social Security numbers to authenticate their accounts when accessing their information online.[625] In FY 2014, the IG determined that this kind of authentication was required on Federal Student Aid websites.[626] The use of Social Security numbers in this way increases "the risk of PII exposure and ultimately identity theft."[627]

The U.S. Department of Education's Federal Information Security Management Act of 2002 Report for Fiscal Year 2014, 39 (Nov. 2014); Office of Inspector General, U.S. Dep't of Education, ED-OIG/A11R0001, The U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2017, 15 (Oct. 2017).

[620] Office of Inspector General, U.S. Dep't of Education, ED-OIG/A11R0001, The U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2017, 15 (Oct. 2017).

[621] *Id.*

[622] *Id.*

[623] Office of Inspector General, U.S. Dep't of Education, 2008 Annual FISMA Report, 8 (Oct. 2009); Office of Inspector General, U.S. Dep't of Education, 2009 Annual FISMA Report, 12 (Oct. 2009); Office of Inspector General, U.S. Dep't of Education, 2010 Annual FISMA Report, 3 (Oct. 2010); Office of Inspector General, U.S. Dep't of Education, ED-OIG/A11L0003, The U.S. Department of Education's Federal Information Security Management Act of 2002 Report for Fiscal Year 2011, 21 (Oct. 2011); Office of Inspector General, U.S. Dep't of Education, ED-OIG/A11N0001, The U.S. Department of Education's Federal Information Security Management Act of 2002 Report for Fiscal Year 2013, 17 (Nov. 2013); Office of Inspector General, U.S. Dep't of Education, ED-OIG/A11O0001, The U.S. Department of Education's Federal Information Security Management Act of 2002 Report for Fiscal Year 2014, 18 (Nov. 2014); Office of Inspector General, U.S. Dep't of Education, ED-OIG/A11R0001, The U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2017, 21 (Oct. 2017); Office of Inspector General, U.S. Dep't of Education, ED-OIG/A11S0001, The U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2018, 28 (Oct. 31, 2018).

[624] Office of Inspector General, U.S. Dep't of Education, ED-OIG/A11R0001, The U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2017, 21 (Oct. 2017).

[625] Office of Inspector General, U.S. Dep't of Education, ED-OIG/A11O0001, The U.S. Department of Education's Federal Information Security Management Act of 2002 Report for Fiscal Year 2014, 18 (Nov. 2014).

[626] *Id.*

[627] *Id.*

4. CIO Turnover and OCIO Challenges

Between 2012 and 2017, the Department only had two CIOs.[628] The current Education CIO has been in office for just over three years.[629] Among the agencies discussed here, this ranks as the longest CIO tenure by nearly a year.

Notwithstanding Education's relative CIO stability, the OCIO has experienced considerable leadership issues as recently as 2016. In 2016, the Education IG investigated then-CIO Danny Harris for improperly awarding Department contracts to a personal friend, operating a side business employing OCIO subordinate employees, and obtaining Department employment for a relative.[630] The Education IG's investigation report detailed Harris's misuse of his position and found that Harris used his Department email for his outside business ventures and made a personal loan to subordinate staff.[631] Improper supervisor relationships with subordinate staff can create circumstances in which "it may appear to a reasonable person that [the supervisor] cannot be impartial with respect to decisions about promotions, bonuses, or assignments."[632] The investigation concluded with the Education IG making a criminal referral to the IRS for failure to report all of his income.[633] In spite of these findings, and the OCIO's lackluster performance, the Department awarded Mr. Harris bonuses in excess of $200,000 over ten years.[634]

5. IT Spending on Operations and Maintenance

For FY 2018, Education requested $745 million for information technology, with the expectation of devoting $619 million to O&M.[635] This amounts to roughly 83 percent of the Department's overall IT budget request. The Department was

---

[628] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 18-93, FEDERAL INFORMATION OFFICERS: CRITICAL ACTIONS NEEDED TO ADDRESS SHORTCOMINGS AND CHALLENGES IN IMPLEMENTING RESPONSIBILITIES, 74 (AUG. 2018).
[629] *Senior Staff*, U.S. Dep't of Education, (Sept. 6, 2016), https://www2.ed.gov/news/staff/bios/gray.html.
[630] *U.S. Dep't of Education: Investigation of the CIO Before the H.Comm. on Oversight & Govt. Reform*, 114th Cong. (2016) (statement of Deputy Inspector General Sandra D. Bruce, U.S. Dep't of Educ.).
[631] U.S. Dep't of Education, Response to Addendum to the Report Investigation: ED/OIG Case: #11-000468, Danny Harris (2015).
[632] U.S. Dep't of Education, Memo to CIO Danny Harris on Ethics Guidance, (July 9, 2015).
[633] U.S. Dep't of Education, Response to Addendum to the Report Investigation: ED/OIG Case: #11-000468, Danny Harris (2015).
[634] *U.S. Dep't of Education: Investigation of the CIO Before the H.Comm. on Oversight & Govt. Reform*, 114th Cong. 3 (2016) (statement of Rep. Jason Chaffetz, Chairman, U.S. House of Rep. Comm. on Oversight & Govt. Reform).
[635] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 18-93, FEDERAL INFORMATION OFFICERS: CRITICAL ACTIONS NEEDED TO ADDRESS SHORTCOMINGS AND CHALLENGES IN IMPLEMENTING RESPONSIBILITIES, 74 (AUG. 2018).

unable to provide the Subcommittee with the precise amount of O&M spending that it devoted to the maintenance of legacy systems.[636]

H. The Social Security Administration

The Social Security Administration ("SSA") provides benefits to over 64 million Americans including retirees, children, widows, and widowers.[637] SSA is charged with protecting some of the most sensitive personal and financial information of American citizens.[638]

1. Examples of Information Held by the Social Security Administration

SSA routinely exchanges "PII and other sensitive information with the public."[639] This information typically includes names, dates and places of birth, medical information, Social Security numbers, financial and employment information, and educational information.[640] As described by one auditor, the PII held by SSA consists of "every type you could imagine."[641]

To conduct its everyday business, SSA maintains a number of systems, databases, and data files (i.e. master data) containing this information. SSA uses several of these to manage Title II (Retirement, Survivors, or Disability Insurance) Social Security benefits and Medicare Enrollments and handles "all post-adjudicative entitlement and payment activities for individuals entitled to Title II benefits."[642] To do so, the Title II systems collect information "such as names, dates of birth, Social Security numbers, and marital status."[643] Moreover, the Title II system also collects "data related to earnings and Supplemental Security Income for the aged, blind, and disabled; data from the Centers for Medicare and Medicaid Services; and data from the Railroad Retirement Board."[644] Finally, to qualify for Title II Disability insurance, claimants must submit health records describing their "impairment(s), treatment sources, and other information that relates to the alleged disability."[645]

---

[636] Email from U.S. Dep't of Education to Subcommittee staff (May 30, 2019) (On file with Subcommittee).
[637] *About Us*, U.S. Social Security Administration, https://www.ssa.gov/agency/.
[638] *Id.*
[639] Office of Inspector General, U.S. Social Security Administration, A-01-13-13025, Sensitive Information at Social Security Administration Offices, 1 (Oct. 18, 2013).
[640] *Id.* at 5.
[641] Briefing with the U.S. Social Security Administration, Office of Inspector General (Nov. 9, 2018).
[642] U.S. Social Security Administration, 016-00-SSA/DCS-M-001, Privacy Impact Assessment Title II System, (Sept. 27, 2007).
[643] *Id.*
[644] *Id.*
[645] *Disability Evaluation Under Social Security*, U.S. Social Security Administration, https://www.ssa.gov/disability/professionals/bluebook/index.htm.

Another database is the e-Authentication File—SSA collects PII as a means of identity verification.[646] Once a user's identity is verified through the e-Authentication file, he or she is permitted "to conduct business with [SSA] electronically."[647] The PII collected for the e-Authentication file includes names, addresses, dates of birth, Social Security numbers, and telephone numbers.[648]

Another example of sensitive data collected is SSA's Earning Record Maintenance System ("ERMS"). ERMS "receives earnings data from employers and self-employed individuals and processes that earnings data to [SSA's] Master Earnings File."[649] This Master Earnings File documents the earning histories "for each of the 350+ million Social Security numbers that have been assigned to workers."[650] SSA uses these earning histories to determine eligibility for Title II and Title XVII benefits under the Social Security Act.[651]

2. FY 2018 Inspector General FISMA Report

The SSA IG contracted with private accounting and consulting firm Grant Thornton to determine whether SSA's overall information security program and practices were effective and consistent with FISMA requirements. Grant Thornton determined that SSA's information security program was ineffective in all five NIST security functions.[652]

Use of Unsupported Systems. Grant Thornton determined that SSA's legacy case processing system for Disability Determination Services ("DDS") had "issues with logical access controls that could result in inappropriate or unauthorized access."[653] Moreover, the IG found that SSA consolidated all regional office DDS case processing systems into a single authority to operate, creating the risk that SSA "did not appropriately document system boundaries."[654] Failure to appropriately document these boundaries can lead to the "improper implementation and execution of security assessment and authorization processes."[655]

---

[646] U.S. Social Security Administration, Privacy Impact Assessment Central Repository of Electronic Authentication Data Master File, (June 2, 2011).
[647] *Id.*
[648] *Id.*
[649] U.S. Social Security Administration, 016-00-SSA/DCS-M-004, Privacy Impact Assessment Earnings Record Maintenance System (Sept. 27, 2007).
[650] *Id.*
[651] *Id.*
[652] Office of Inspector General, U.S. Social Security Administration, A-14-18-50505, The Social Security Administration's Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2018, 5 (Oct. 31, 2018).
[653] *Id.* at 8.
[654] *Id.* at 6.
[655] *Id.*

Failure to Remediate Vulnerabilities. Although Grant Thornton determined that SSA had defined a configuration management plan, they also found that "high risk vulnerabilities remained on the network due to missing patches that were not remediated in a timely fashion."[656] In addition, SSA did not document a policy for how internet protocol phones and network devices "should be configured or how to ensure devices should use current software with the appropriate patches."[657]

Failure to Compile an Accurate and Comprehensive IT Asset Inventory. SSA also failed to implement an "inventory of related hardware and software components at a level of granularity necessary for tracking and reporting to management."[658] SSA's inventory did not include all of its information systems pursuant to NIST standards.[659] The SSA IG first identified this issue in 2014 and 2015 and continued to highlight it in recent annual FISMA audits.[660] An incomplete inventory presents the risk that software could be operating on SSA's network without the knowledge of IT personnel.[661] Consequently, if a hostile actor chose to exploit an unknown application, the ability for the agency to respond to the cyber-attack would be significantly hindered as security personnel attempted to locate the source of the breach.[662] SSA should create and maintain an up-to-date and accurate inventory listing all IT assets. This would provide the visibility necessary to aid the agency in responding to a cyber-attack.

Failure to Provide for the Adequate Protection of PII. Nation state cyber-attackers frequently target SSA because of the substantial quantities of PII it maintains.[663] This fact further underscores the importance of SSA efforts to better protect sensitive information in its custody.[664] The most troubling findings in the latest SSA FISMA audit were the weaknesses identified in identity and access management. Although SSA established an Agency-wide information security program and practices, Grant Thornton identified a number of weaknesses similar to the deficiencies reported in past FISMA performance audits—including issues related to identity and access management.[665]

Additional Cybersecurity Issues. Recently, SSA attempted to improve its security training protocols by removing internet access for those who do not complete annual training requirements.[666] Nevertheless, Grant Thornton noted

---

[656] *Id.* at B-10.
[657] *Id.* at 8.
[658] *Id.* at 7.
[659] *Id.* at B-3.
[660] Briefing with the U.S. Social Security Administration, Office of Inspector General (Nov. 9, 2018).
[661] *Id.*
[662] *Id.*
[663] *Id.*
[664] *Id.*
[665] Email from U.S. Social Security Administration to Subcommittee staff (June 19, 2019) (On file with Subcommittee).
[666] Briefing with the U.S. Social Security Administration, Office of Inspector General (Nov. 9, 2018).

that "the SSA Learning Management System contained weaknesses that did not require users to fully complete training material before they received credit for completing the course."[667]

3. Persistent Problems Based on Prior IG FISMA Audits

Lack of Valid Authorities to Operate. FY 2014, 2015, 2016, and 2017 FISMA audits determined that SSA maintained systems lacking valid authorities to operate.[668] In particular, SSA struggled to ensure "that third-party information security controls were measured, reported, and monitored."[669] For example, auditors found that "Authorizations to Operate were unavailable for some systems managed by contractors or external service providers."[670]

Failure to Remediate Vulnerabilities. FISMA audits in *six* of the past *eleven* fiscal years found that SSA had deficiencies regarding the timely installation of software patches.[671] Auditors determined that SSA "has developed, documented, and disseminated its policies and procedures for flaw remediation, including patch

---

[667] Office of Inspector General, U.S. Social Security Administration, A-14-18-50505, The Social Security Administration's Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2018, 9 (Oct. 31, 2018).

[668] Office of Inspector General, U.S. Social Security Administration, 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 (Oct. 2014); Office of Inspector General, U.S. Social Security Administration, 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 (Nov. 2015); Office of Inspector General, U.S. Social Security Administration, 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 (Nov. 2016); Office of Inspector General, U.S. Social Security Administration, A-14-18-50258, The Social Security Administration's Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2017, 7 (Oct. 2017).

[669] Office of the Inspector General, U.S. Social Security Administration, A-14-18-50258, The Social Security Administration's Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2017, 7 (Oct. 2017).

[670] *Id.*

[671] Office of Inspector General, U.S. Social Security Administration, A-14-09-19047, Fiscal Year 2009 Evaluation of the Social Security Administration's Compliance with the Federal Information Security Management Act, 8 (Nov. 2009); Office of Inspector General, U.S. Social Security Administration, A-14-10-20109, Fiscal Year 2010 Evaluation of the Social Security Administration's Compliance with the Federal Information Security Management Act, 14−15 (Nov. 2010); Office of Inspector General, U.S. Social Security Administration, A-14-13-13086, The Social Security Administration's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2013, B-3 (Nov. 2013); Office of Inspector General, U.S. Social Security Administration, A-14-17-50151, The Social Security Administration's Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2016, B-8 (Nov. 2016); Office of Inspector General, U.S. Social Security Administration, A-14-18-50258, The Social Security Administration's Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2017, B-9 (Oct. 2017); Office of Inspector General, U.S. Social Security Administration, A-14-18-50505, The Social Security Administration's Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2018, B-10 (Oct. 31, 2018).

management," but vulnerability assessments and IT diagnostic security testing found instances where patches were not installed.[672]

Failure to Compile an Accurate & Comprehensive IT Asset Inventory. Auditors noted SSA's failure to compile an accurate IT asset inventory in *seven* of the last *eleven* fiscal years.[673] Moreover, the IG highlighted this issue in four consecutive FISMA audits beginning in FY 2015.[674] While SSA has started to implement automated tools to track software and hardware assets, auditors have consistently found that its inventory "was incomplete and inaccurate, did not include some contractor systems, and did not distinguish external systems" in accordance with NIST and OMB standards.[675]

Failure to Provide for the Adequate Protection of PII. Auditors determined that SSA failed to adequately protect PII *eight* times over the last *eleven* years.[676]

---

[672] Office of the Inspector General, U.S. Social Security Administration, A-14-18-50258, The Social Security Administration's Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2017, B-9 (Oct. 2017).

[673] Office of Inspector General, U.S. Social Security Administration, A-14-10-20109, Fiscal Year 2010 Evaluation of the Social Security Administration's Compliance with the Federal Information Security Management Act, 6 (Nov. 2010); Office of Inspector General, U.S. Social Security Administration, A-14-11-01134, Fiscal Year 2011 Evaluation of the Social Security Administration's Compliance with the Federal Information Security Management Act of 2002, 14−15 (Nov. 2011); Office of Inspector General, U.S. Social Security Administration, A-14-12-12120, The Social Security Administration's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2012, 6-7 (Nov. 2012); Office of Inspector General, U.S. Social Security Administration, A-14-16-50037, The Social Security Administration's Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2015, B-9 (Nov. 2015); Office of Inspector General, U.S. Social Security Administration, 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 (Nov. 2016); Office of Inspector General, U.S. Social Security Administration, A-14-18-50258, The Social Security Administration's Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2017, 6 (Oct. 2017); Office of Inspector General, U.S. Social Security Administration, A-14-18-50505, The Social Security Administration's Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2018, 7 (Oct. 31, 2018).

[674] Briefing with the U.S. Social Security Administration, Office of Inspector General (Nov. 9, 2018); Office of Inspector General, U.S. Social Security Administration, A-14-16-50037, The Social Security Administration's Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2015, B-9 (Nov. 2015); Office of Inspector General, U.S. Social Security Administration, 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 (Nov. 2016); Office of Inspector General, U.S. Social Security Administration, A-14-18-50258, The Social Security Administration's Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2017, 6 (Oct. 2017); Office of Inspector General, U.S. Social Security Administration, A-14-18-50505, The Social Security Administration's Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2018, 7 (Oct. 31, 2018).

[675] Office of the Inspector General, U.S. Social Security Administration, A-14-18-50258, The Social Security Administration's Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2017, B-2, B-3 (Oct. 2017).

[676] Office of Inspector General, U.S. Social Security Administration, A-14-08-18063, Fiscal Year 2008 Evaluation of the Social Security Administration's Compliance with the Federal Information

Over this time period, SSA's deficiencies can be partially attributed to its failure to more fully restrict access to databases that contain PII.[677] Recent penetration testing identified issues related to monitoring and responding to cybersecurity threats.[678]

4. CIO Turnover and OCIO Challenges

SSA has also had trouble with the retention of its CIO's. Between 2012 and 2017, SSA had six different CIOs.[679] SSA's current CIO has been in office for approximately two years; he started in June 2017.[680]

A 2018 GAO report found that SSA departmental policies largely failed to document how the CIO leads IT strategic planning.[681] As a result, department policies did not clearly outline how the CIO is to promote greater FISMA compliance by improving agency operations through IT.[682] SSA policies did not require that the CIO report annually to the agency head on improvements made to IT personnel or

---

Security Management Act, 4 (Sept. 2008); Office of Inspector General, U.S. Social Security Administration, A-14-09-19047, Fiscal Year 2009 Evaluation of the Social Security Administration's Compliance with the Federal Information Security Management Act, 7–8 (Nov. 2009); Office of Inspector General, U.S. Social Security Administration, A-14-10-20109, Fiscal Year 2010 Evaluation of the Social Security Administration's Compliance with the Federal Information Security Management Act, 9–10 (Nov. 2010); Office of Inspector General, U.S. Social Security Administration, A-14-11-01134, Fiscal Year 2011 Evaluation of the Social Security Administration's Compliance with the Federal Information Security Management Act of 2002, 9 (Nov. 2011); Office of Inspector General, U.S. Social Security Administration, A-14-12-12120, The Social Security Administration's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2012, 7–8 (Nov. 2012); [676] Office of Inspector General, U.S. Social Security Administration, A-14-17-50151, The Social Security Administration's Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2016, 7 (Nov. 2016); Office of Inspector General, U.S. Social Security Administration, 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 (Oct. 2017); Office of Inspector General, U.S. Social Security Administration, A-14-18-50505, The Social Security Administration's Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2018, 8, B-18 (Oct. 31, 2018).

[677] Office of the Inspector General, U.S. Social Security Administration, A-14-17-50151, The Social Security Administration's Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2016, 7 (Nov. 2016).

[678] Office of the Inspector General, U.S. Social Security Administration, 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 (Oct. 2017).

[679] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 18-93, FEDERAL INFORMATION OFFICERS: CRITICAL ACTIONS NEEDED TO ADDRESS SHORTCOMINGS AND CHALLENGES IN IMPLEMENTING RESPONSIBILITIES, 112 (AUG. 2018).

[680] Adam Mazmanian, *SSA gets new CIO*, FEDERAL COMPUTER WEEK, June 7, 2017, https://fcw.com/blogs/fcw-insider/2017/06/ssa-cio.aspx.

[681] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 18-93, FEDERAL INFORMATION OFFICERS: CRITICAL ACTIONS NEEDED TO ADDRESS SHORTCOMINGS AND CHALLENGES IN IMPLEMENTING RESPONSIBILITIES, 112 (AUG. 2018).

[682] *Id.*

that the CIO annually develop strategies to rectify IT staff deficiencies.[683] Since that GAO report, SSA has issued an agency directive addressing these concerns and more completely documenting the role of its CIO.[684]

5. IT Spending on Operations and Maintenance

SSA devotes a majority of its IT funds to O&M. In FY 2018, SSA submitted an overall IT budget request of nearly $1.7 billion.[685] SSA estimated that it would need $1.1 billion of that total request for O&M—roughly 66 percent of its total IT budget request.[686] SSA was unable to provide the Subcommittee with the precise amount of O&M spending that it devoted to the maintenance of legacy systems.[687]

One example of an expensive SSA system that adds to O&M spending is SSA's legacy Title II system first introduced 34 years ago.[688] As mentioned above, this is the system "which determines retirement benefits eligibility and amounts."[689] In describing the system, SSA officials noted that Title II has a total of 162 subsystems—some that are still written in COBOL.[690] One leading IT research group suggested that organizations using COBOL should reconsider because "operating costs will steadily rise, and because there is a decrease in people available with the proper skill sets."[691] SSA officials confirmed this saying "that most of the employees who developed these systems are ready to retire and the agency will lose their collective knowledge."[692] In 2017, SSA started a campaign to modernize its oldest legacy systems including Title II.[693] For Title II, SSA developed a five-year modernization roadmap that is scheduled through FY 2022.[694]

---

683 *Id.*
684 Email from U.S. Social Security Administration to Subcommittee staff (Jun. 7, 2019) (On file with Subcommittee).
685 *Id.*
686 *Id.*
687 Email from U.S. Social Security Administration to Subcommittee staff (Jun. 3, 2019) (On file with Subcommittee).
688 U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 16-468, INFORMATION TECHNOLOGY: FEDERAL AGENCIES NEED TO ADDRESS AGING LEGACY SYSTEMS, 62 (MAY 2016).
689 *Id.*
690 *Id.*
691 *Id.* at 57.
692 *Id.* at 62.
693 Email from U.S. Social Security Administration to Subcommittee staff (Apr. 2, 2019) (On file with Subcommittee).
694 *Id.*

V. CONCLUSION

Despite major data breaches like OPM, the federal government remains unprepared to confront the dynamic cyber threats of today. The longstanding cyber vulnerabilities consistently highlighted by Inspectors General illustrate the federal government's failure to meet basic cybersecurity standards to protect sensitive data. The Subcommittee will continue to track federal agency cybersecurity to ensure agencies meet FISMA's primary legislative objective to secure government information systems.