United States Government Accountability Office

Before the Subcommittee on Technology Modernization, Committee on Veterans' Affairs, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. ET
Thursday, November 14, 2019

INFORMATION SECURITY

VA and Other Federal Agencies Need to Address Significant Challenges

Statement of Gregory C. Wilshusen,
Director, Information Security Issues

Accessible Version

GAO-20-256T

GAO Highlights

Highlights of GAO-20-256T, a testimony before the Subcommittee on Technology Modernization, Committee on Veterans' Affairs, House of Representatives

November 14, 2019

INFORMATION SECURITY

VA and Other Federal Agencies Need to Address Significant Challenges

Why GAO Did This Study

In providing health care and other benefits to veterans and their dependents, VA relies extensively on IT systems and networks to receive, process, and maintain sensitive data, including veterans' medical records and other personally identifiable information. Accordingly, effective security controls based on federal guidance and requirements are essential to ensure that VA's systems and information are adequately protected from loss, unauthorized disclosure, inadvertent or deliberate misuse, or improper modification, and are available when needed.

For this testimony, GAO summarized the status of information security across the federal government and particularly at VA. It also discusses the security challenges that VA faces as it modernizes and secures its information systems. To develop this statement, GAO reviewed its prior reports and relevant Office of Management and Budget, IG, and agency reports.

What GAO Recommends

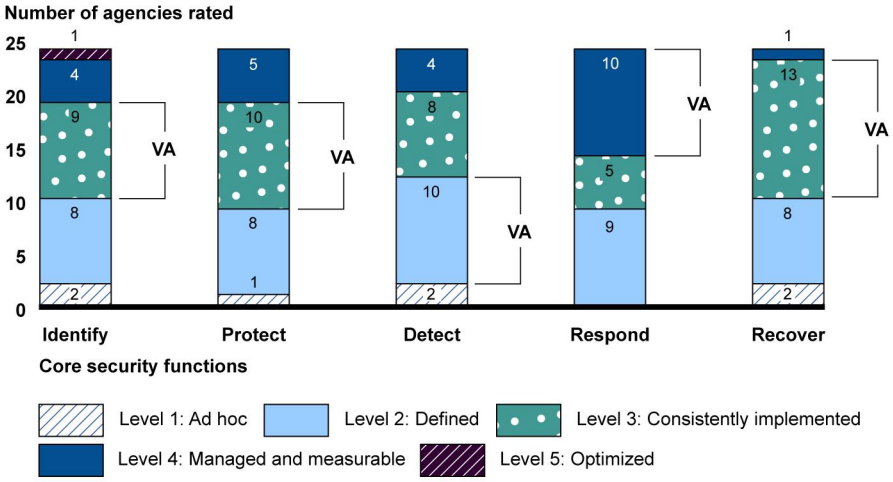
In 2016, GAO recommended 74 actions for VA to take to address deficiencies and improve its cybersecurity program. However, as of October 2019, VA had not demonstrated that it had addressed 42 of these recommendations. In 2019, GAO made four additional recommendations to improve the department's cybersecurity risk management program and one recommendation to accurately identify work roles of IT and cybersecurity workforce positions. VA concurred with

View GAO-20-256T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Federal agencies, including the Department of Veterans Affairs (VA), continue to have deficient information security programs. For example, in fiscal year 2018, inspectors general (IGs) used a five-level maturity model to rate agency information security policies, procedures, and practices related to the five core security functions—*identify*, *protect*, *detect*, *respond*, and *recover*—established by the National Institute of Standards and Technology's cybersecurity framework. VA's ratings were generally consistent with the ratings of other major agencies (see figure) and its information security program was one of 18 agency programs that IGs deemed ineffective.

Maturity Level Ratings for the Cybersecurity Framework Core Security Functions for 24 Major Agencies, including the Department of Veterans Affairs (VA), for Fiscal Year 2018



Source: GAO analysis of agency fiscal year 2018 *Federal Information Security Modernization Act of 2014* (FISMA) reports and the Office of Management and Budget's *Fiscal Year 2018 Annual FISMA Report to Congress.* | GAO-20-256T

Data Table for Maturity Level Ratings for the Cybersecurity Framework Core Security Functions for 24 Major Agencies, including the Department of Veterans Affairs (VA), for Fiscal Year 2018

	Level 1: Ad hoc	Level 2: Defined	Level 3: Consistently implemented	Level 4: Managed and measurable	Level 5: Optimized
Identify	2	8	9	4	1
Protect	1	8	10	5	0
Detect	2	10	8	4	0
Respond	0	9	5	10	0
Recover	2	8	13	1	0

Most major agencies, including VA, had significant security control deficiencies over their financial reporting. For example, for fiscal year 2018, VA's IG reported deficiencies in control areas, such as security management, access control,

configuration management, segregation of duties, and contingency planning. Additionally, as of fiscal year 2018, VA reported meeting six of the 10 cybersecurity performance targets set by the administration.

VA faces several security challenges as it secures and modernizes its information systems. These challenges pertain to effectively implementing information security controls; mitigating known vulnerabilities; establishing elements of its cybersecurity risk management program; and identifying critical cybersecurity staffing needs. VA also faces the additional challenge of managing IT supply chain risks as the department takes steps to modernize its information systems.

Chair Lee, Ranking Member Banks, and Members of the Subcommittee

Thank you for the opportunity to testify at today's hearing on cybersecurity challenges and cyber risk management at the Department of Veterans Affairs (VA). As you know, federal agencies, including VA, rely extensively on information technology (IT) to carry out their operations and deliver services to constituents.

Safeguarding federal computer systems has been a longstanding concern. This year marks the 22nd anniversary of GAO's first designation of information security as a government-wide high-risk area in 1997.[1] We expanded this high-risk area to include safeguarding the systems supporting our nation's critical infrastructure in 2003, protecting the privacy of personally identifiable information in 2015, and establishing a comprehensive cybersecurity strategy and performing effective oversight in 2018.[2] Most recently, we identified federal information security as a government-wide high-risk area in our March 2019 high-risk update.[3]

As we agreed, my statement provides an overview of the status of cybersecurity across the federal government in general and at VA in particular. This includes a discussion of the IT security challenges that the department faces as it modernizes and secures its information systems.

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

[2]GAO, *High-Risk Series: Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructures*, GAO-03-121 (Washington, D.C.: January 2003); *High-Risk Series: An Update*, GAO-15-290 (Washington, D.C.: February 11, 2015); and *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation*, GAO-18-622 (Washington, D.C.: September 6, 2018).

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

In developing this testimony, we reviewed our prior reports,[4] as well as relevant Office of Management and Budget (OMB), inspector general (IG), and agency reports. A more detailed discussion of the objectives, scope, and methodology for this work is included in each of the reports that are cited throughout this statement.

The work on which this statement is based was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform audits to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions. We believe that the evidence obtained provided a reasonable basis for our findings and conclusions based on our audit objectives.

Background

VA's mission is to promote the health, welfare, and dignity of all veterans by ensuring that they receive medical care, benefits, social support, and lasting memorials. In providing health care and other benefits to veterans and their dependents, VA relies extensively on IT systems and networks to receive, process, and maintain sensitive data, including veterans' medical records and other personally identifiable information. Accordingly, effective information security controls based on federal guidance and requirements are essential to ensure that the department's systems and information are adequately protected from loss, unauthorized disclosure, inadvertent or deliberate misuse, or improper modification, and are available when needed.

Implementing an effective information security program and controls is particularly important for VA since it uses IT systems and electronic information to perform essential activities for veterans, such as providing primary and specialized health care services, medical research, disability

[4]See, for example, GAO, *Federal Information Security: Agencies and OMB Need to Strengthen Policies and Practices*, GAO-19-545 (Washington, D.C.: July 26, 2019); *Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges*, GAO-19-384 (Washington, D.C.: July 25, 2019); *Cybersecurity Workforce: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs*, GAO-19-144 (Washington, D.C: March 12, 2019); *Information Security: Supply Chain Risks Affecting Federal Agencies*, GAO-18-667T (Washington, D.C.: July 12, 2018); *Information Security: VA Needs to Improve Controls over Selected High-Impact Systems*, GAO-16-691SU (Washington, D.C.: September 30, 2016); and *Information Security: Agencies Need to Improve Controls over Selected High-Impact Systems*, GAO-16-501 (Washington, D.C.: May 18, 2016).

compensation, educational opportunities, assistance with home ownership, and burial and memorial benefits. The corruption, denial, or delay of these services due to compromised IT systems and electronic information can create undue hardship for veterans and their dependents.

Federal Law and Policy Set Requirements for Securing Federal Systems and Information

The *Federal Information Security Modernization Act of 2014* (FISMA) requires the head of each agency to provide information security protections commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of the information and information systems used by or on behalf of the agency. The act also requires federal agencies to develop, document, and implement an agency-wide information security program to provide security for the information and information systems supporting their operations and assets by implementing policies and procedures intended to cost-effectively reduce risks to an acceptable level.[5]

In May 2017, the president signed Executive Order 13800 on strengthening the cybersecurity of federal networks and critical infrastructure.[6] The order sets policy for managing cybersecurity risk and directs each executive branch agency to use the National Institute of Standards and Technology's (NIST) cybersecurity framework to manage those risks.[7]

The NIST cybersecurity framework identifies specific activities and controls for achieving five core security functions:

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

[6]White House, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, Executive Order 13800 (Washington, D.C.: May 11, 2017).

[7]National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Gaithersburg, MD: Apr. 16, 2018).

- **Identify:** Develop an understanding of the organization's ability to manage cybersecurity risk to systems, people, assets, data, and capabilities.
- **Protect:** Develop and implement appropriate safeguards to ensure delivery of critical services.
- **Detect:** Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
- **Respond:** Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
- **Recover:** Develop and implement appropriate activities to maintain plans for resilience and to restore capabilities or services that were impaired due to a cybersecurity incident.

According to NIST, these five functions provide a high-level, strategic view of the life cycle of an organization's management of cybersecurity risk.

The 23 Civilian CFO Act Agencies Have Spent Billions on Cybersecurity Activities

In fiscal year 2018, the 23 civilian agencies covered by the *Chief Financial Officers Act of 1990* (CFO Act),[8] including VA, reported spending over $6.5 billion on IT security- or cybersecurity-related activities. The 23 civilian agencies individually reported spending between $9 million and almost $1.9 billion on these activities.[9] Collectively, these 23 agencies spent on average about 14 percent of their total IT expenditures on cybersecurity-related activities. VA reported spending

[8]The 23 civilian *Chief Financial Officers Act of 1990* (CFO Act) are the Departments of Agriculture, Commerce, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulation Commission; Office of Personnel Management; Small Business Administration; Social Security Administration; and the U.S. Agency for International Development. In addition to the 23 civilian CFO Act agencies, the Department of Defense is the 24th agency covered by the CFO Act.

[9]According to the President's budget request for fiscal year 2020, the agency-reported cybersecurity spending may include cybersecurity-related spending that was not dedicated to the protection of their networks. Instead, the amounts reported may represent spending for the broader cybersecurity mission of the agency.

about $386 million on cybersecurity, which represented about 8 percent of its total IT expenditures.[10]

Federal Agencies Continue to Report Large Numbers of Security Incidents, Although VA Has Reported Fewer Incidents In Recent Years

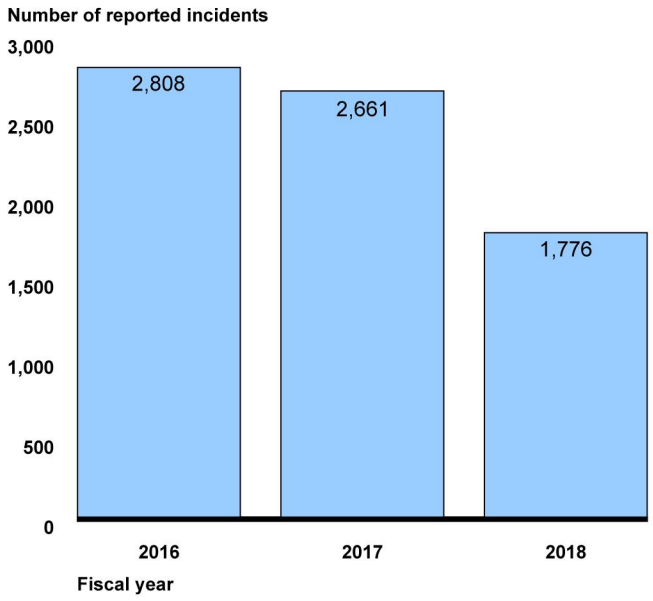
In fiscal year 2018, federal agencies continued to report large numbers of information security incidents. As we previously noted,[11] federal agencies reported over 30,000 security incidents during each of the last three fiscal years. Specifically, agencies reported a total of 30,899, 35,277, and 31,107 information security incidents in fiscal years 2016, 2017, and 2018, respectively. During those same periods of time, VA reported an average of 2,415 incidents annually, although the number of reported incidents steadily decreased from 2,808 to 1,776, as shown in figure 1.[12]

[10]See GAO-19-545.

[11]GAO-19-545.

[12]Office of Management and Budget, *Federal Information Security Modernization Act of 2014 Annual Report to Congress* (Washington, D.C.: June 28, 2019).

Figure 1: Information Security Incidents Reported by the Department of Veterans Affairs, Fiscal Years 2016 through 2018



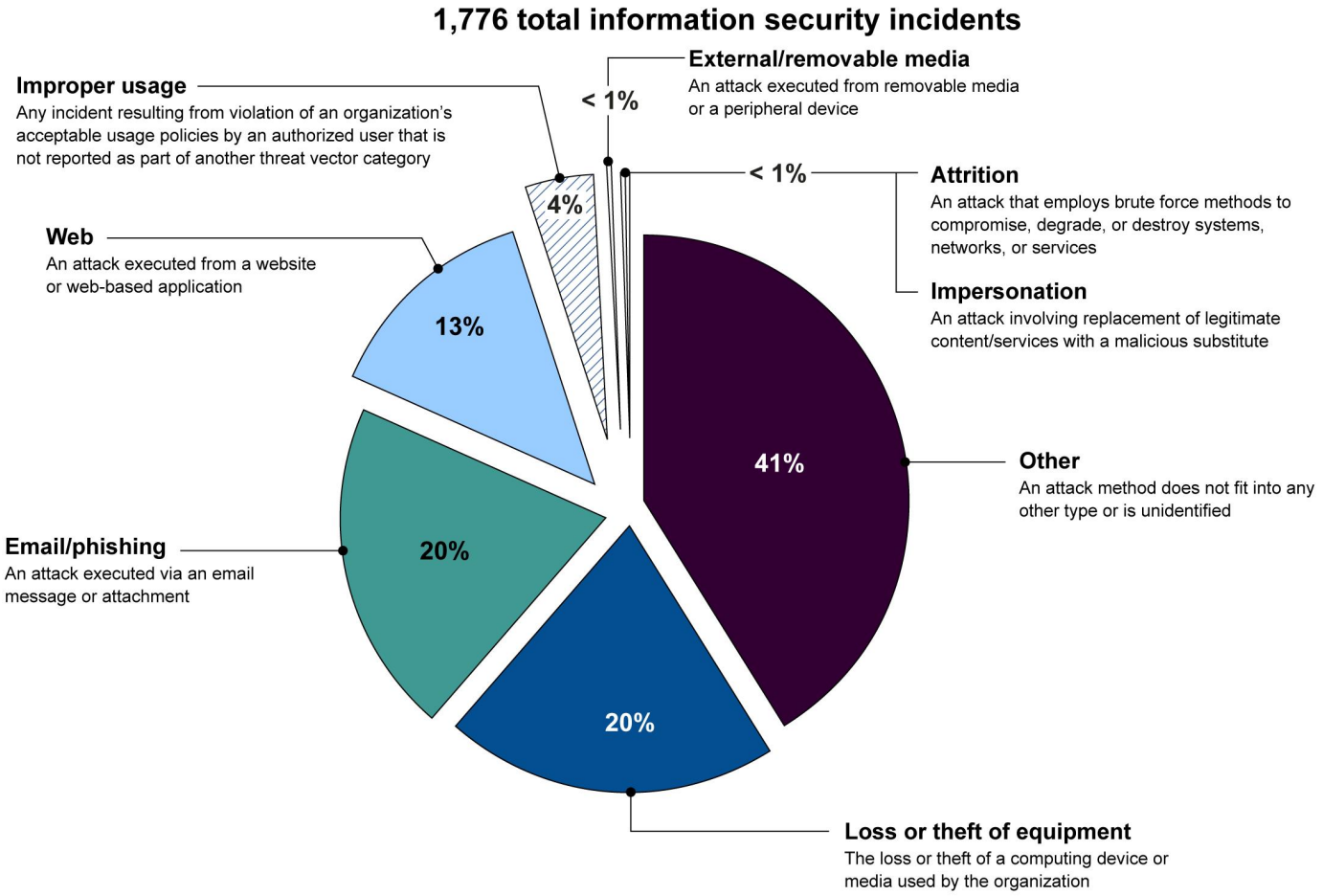
Source: GAO analysis of Office of Management and Budget data. | GAO-20-256T

In fiscal year 2018, VA reported 1,776 incidents involving several threat vectors.[13] These threat vectors included web-based attacks, phishing attacks,[14] and the loss or theft of computer equipment, among others. Figure 2 provides a breakdown of information security incidents, by threat vector, reported by VA in fiscal year 2018.

[13]A threat vector (or avenue of attack) specifies the conduit or means used by the source or attacker to initiate a cyber attack or incident.

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

Figure 2: Department of Veterans Affairs Information Security Incidents by Threat Vector Category, Fiscal Year 2018



Source: GAO analysis of Office of Management and Budget data for fiscal year 2018. | GAO-20-256T

Data Table for Figure 2: Department of Veterans Affairs Information Security Incidents by Threat Vector Category, Fiscal Year 2018

Other	732
Loss or theft of equipment	362
Email	358
Web	239
Improper usage	75
External/removable media	4
Attrition	3
Impersonation	3

Perhaps most concerning of the incidents reported by VA is the relatively large percentage of incidents (41 percent) for which VA identified “Other” as the threat vector. Government-wide, agencies identified approximately 27 percent of their incidents in the “Other” category in fiscal year 2018. A large percentage of these incidents may indicate a lack of agency awareness and ability to investigate and catalog incidents.

Federal Agencies, Including VA, Continue to Have Deficient Information Security Programs

FISMA requires IGs to determine the effectiveness of their respective agency’s information security programs. To do so, OMB instructed IGs to provide a maturity rating for agency information security policies, procedures, and practices related to the five core security functions—*identify, protect, detect, respond, and recover*—established in the NIST cybersecurity framework, as well as for the agency-wide information security program.

The ratings used to evaluate the effectiveness of agency information security programs are based on a five-level maturity model, as described in table 1.

Table 1: Inspector General Reporting Metrics Maturity Model

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 Measurable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies are collected across the organization and used to assess those policies procedures, and strategies, 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.

Source: GAO analysis of Fiscal Year 2018 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics, Version 1.0.1, May 24, 2018. | GAO-20-256T

According to this maturity model, Level 4 (managed and measurable) represents an effective level of security.[15] Therefore, if an IG rates the agency's information security program at Level 4 or Level 5, then that agency is considered to have an effective information security program.

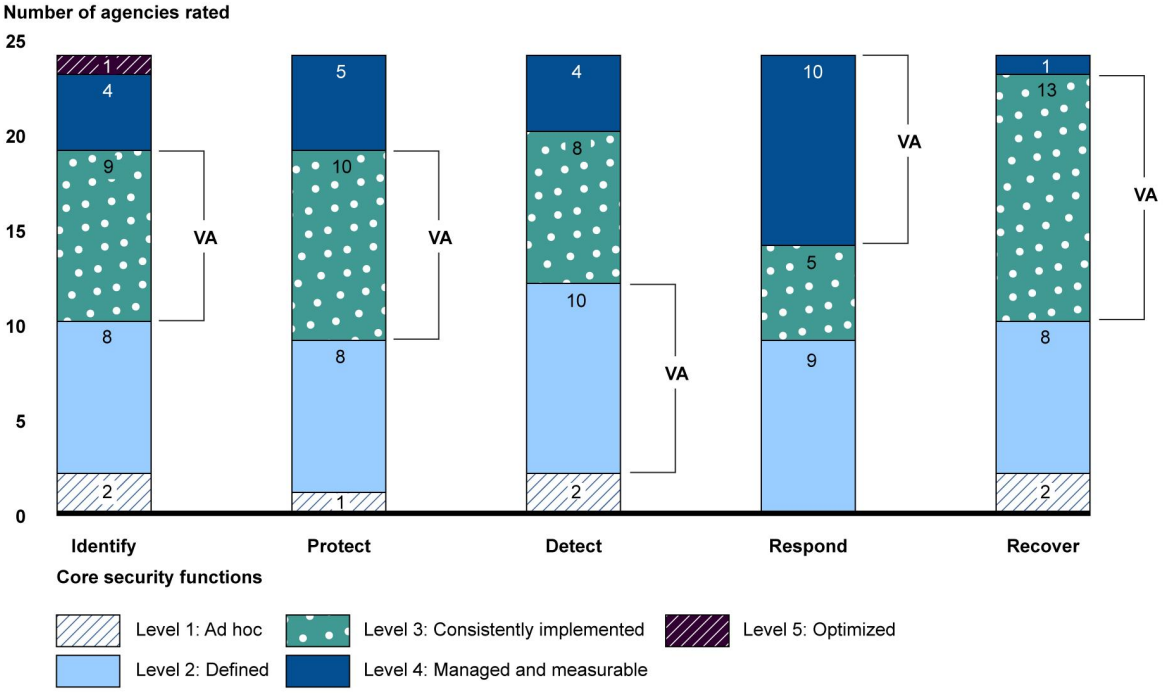
VA was one of 18 CFO Act agencies where the IG determined that the agency-wide information security program was not effectively implemented during fiscal year 2018. The VA IG also determined the department's maturity level for each of the five core security functions:

- Level 2 (defined) for the *Detect* function;
- Level 3 (consistently implemented) for the *Identify, Protect,* and *Recover* functions; and
- Level 4 (managed and measurable) for the *Respond* function.

As shown in figure 3, VA's ratings were generally consistent with the maturity level ratings of other CFO Act agencies.

[15]The National Institute of Standards and Technology defines security control effectiveness as the extent to which security controls are implemented correctly, operate as intended, and produce the desired outcome with respect to meeting the security requirements for the information system and are in compliance with established security policies.

Figure 3: Maturity Level Ratings for the Cybersecurity Framework Core Security Functions for 24 Major Agencies, including the Department of Veterans Affairs (VA), for Fiscal Year 2018



Source: GAO analysis of agency fiscal year 2018 *Federal Information Security Modernization Act of 2014* (FISMA) reports and the Office of Management and Budget's *Fiscal Year 2018 Annual FISMA Report to Congress.* | GAO-20-256T

Data Table for Figure 3: Maturity Level Ratings for the Cybersecurity Framework Core Security Functions for 24 Major Agencies, including the Department of Veterans Affairs (VA), for Fiscal Year 2018

	Level 1: Ad hoc	Level 2: Defined	Level 3: Consistently implemented	Level 4: Managed and measurable	Level 5: Optimized
Identify	2	8	9	4	1
Protect	1	8	10	5	0
Detect	2	10	8	4	0
Respond	0	9	5	10	0
Recover	2	8	13	1	0

Most CFO Act Agencies, Including VA, Had Significant Security Control Deficiencies over Their Financial Reporting

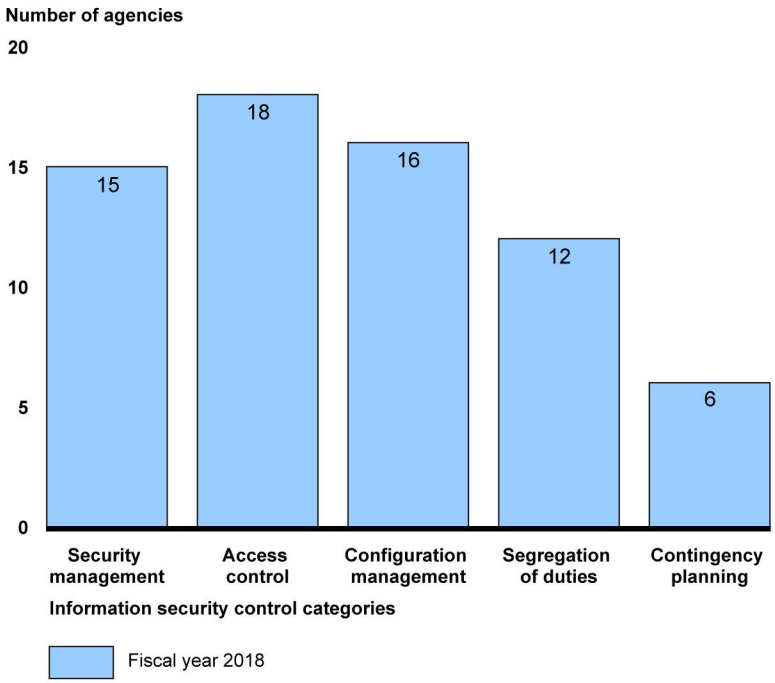
Agency IGs or independent auditors assess the effectiveness of information security controls as part of the annual audits of the agencies' financial statements. The reports resulting from these audits include a description of information security control deficiencies related to the five major general control categories defined by the *Federal Information System Controls Audit Manual* (FISCAM):[16]

- **security management controls** that provide a framework for ensuring that risks are understood and that effective controls are selected, implemented, and operating as intended;
- **access controls** that limit or detect access to computer resources, thereby protecting them against unauthorized modification, loss, and disclosure;
- **configuration management controls** that prevent unauthorized changes to information system resources and assure that software is current and known vulnerabilities are patched;
- **segregation of duties controls** that prevent an individual from controlling all critical stages of a process by splitting responsibilities between two or more organizational groups; and
- **contingency planning controls** that help avoid significant disruptions in computer-dependent operations.

For fiscal year 2018, most of the 24 CFO Act agencies had deficiencies in most of the control categories, as illustrated in figure 4. VA's IG reported deficiencies in each of these categories for the department.

[16]FISCAM is GAO's audit methodology for performing information system control audits in accordance with generally accepted government auditing standards. See GAO, *Federal Information System Controls Audit Manual* (FISCAM), GAO-09-232G (Washington, D.C.: February 2009).

Figure 4: Number of 24 Chief Financial Officers Act of 1990 Agencies Reporting Deficiencies in Information Security Control Categories for Fiscal Year 2018



Source: GAO analysis of agency financial reports for fiscal year 2018. | GAO-20-256T

Data Table for Figure 4: Number of 24 Chief Financial Officers Act of 1990 Agencies Reporting Deficiencies in Information Security Control Categories for Fiscal Year 2018

Year	Number of reported incidents
2016	2808
2017	2661
2018	1776

As a result of these deficiencies, the IGs at 18 of the 24 CFO Act agencies designated information security as either a material weakness (six agencies, including VA) or significant deficiency (12 agencies) in

internal control over financial reporting for their agency.[17] For VA, fiscal year 2018 was the 17th year in a row that the department had reported a material weakness in information security. In addition, IGs at 21 of the 24 agencies, including VA, cited information security as a major management challenge for their agency for fiscal year 2018.

Most Civilian CFO Act Agencies, Including VA, Have Reported Meeting Many Cybersecurity Implementation Targets

The administration has developed key milestones and performance metrics for agency chief information officers (CIO) to use to assess their agency's progress toward achieving outcomes that strengthen federal cybersecurity. The milestones and metrics have specific implementation targets, most of which are expected to be met by the end of fiscal year 2020.

As of fiscal year 2018, most civilian CFO Act agencies, including VA, had reported meeting most of the implementation targets for that year.[18] VA reported meeting six of 10 targets. Table 2 shows the number of agencies meeting their targets as of fiscal year 2018, as well as VA's status in doing so.

[17]A material weakness is a deficiency, or combination of deficiencies, in internal control over financial reporting, such that there is a reasonable possibility that a material misstatement of an entity's financial statement will not be prevented, or detected and corrected on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control over financial reporting that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis.

[18]We did not include the Department of Defense because the data was not publicly available.

Table 2: Number of 23 Civilian Chief Financial Officers Act of 1990 Agencies Meeting Targets for 10 Key Milestones, along with the Department of Veterans Affairs' Status, for Fiscal Year 2018

Key milestone	Performance Metric & Target	Number of agencies reported meeting targets	VA status
Software asset management	95% of software assets are covered by a whitelisting capability.[a]	10	Not met
Hardware asset management	95% of hardware assets are covered by a capability to detect and alert upon the connection of an unauthorized hardware asset.	16	Not met
Authorization management	100% of high and moderate impact systems are covered by a valid security authorization to operate.	14	Not met
Mobile device management	95% of mobile devices are covered by a capability to remotely wipe contents if the device is lost or compromised.	19	Met
Privileged network access management	100% of privileged users are required to use a Personal Identity Verification (PIV) card[b] or Authenticator Assurance Level 3[c] (AAL3) multifactor authentication method to access the agency's network.	18	Met
High-value asset access management	90% of high-value assets require all users to authenticate using a PIV card or AAL3 multifactor authentication method.	14	Met
Automated access management	95% of users are covered by an automated, dynamic access management solution that centrally tracks access and privilege levels.	15	Not met
Intrusion detection and prevention	At least 4 of 6 intrusion prevention metrics have met an implementation target of at least 90% and 100% of email traffic is analyzed using email authentication protocols that prevent malicious actors from sending false emails claiming to originate from a legitimate source.	8	Met
Exfiltration and enhanced defenses	At least 3 of 4 exfiltration and enhanced defenses metrics have met an implementation target of at least 90%.	23	Met
Data protection	At least 4 of 6 data protection metrics have met an implementation target of at least 90%.	16	Met

Source: GAO analysis of Fiscal Year 2018 Chief Information Officer Federal Information Security Modernization Act of 2014 Reporting Metrics | GAO-20-256T

[a]Whitelisting is a process used to identify (1)software programs that are authorized to execute on an information system or (2) authorized websites.

[b]A Personal Identity Verification card is a physical artifact that contains stored identity credentials for the person it was issued to, so that the identity of the individual can be verified against the stored credentials by another person or an automated process.

[c]Authenticator Assurance Level 3 uses a hardware-based authenticator and an authenticator that provides verifier impersonation resistance.

VA Faces Key Security Challenges As It Modernizes and Secures Its Information Systems

In several reports issued since fiscal year 2016, we described deficiencies related to key challenges that VA has faced in safeguarding its information and information systems. The challenges we reported related to effectively implementing information security controls; mitigating known security deficiencies; establishing elements of its cybersecurity risk management program; and identifying critical cybersecurity staffing needs. Our work stresses the need for VA to address these challenges as well as manage IT supply chain risks as it modernizes and secures its information systems.

Effectively Implementing Information Security Controls

VA has been challenged to effectively implement security controls over its information and information systems. As previously mentioned in this statement, the VA IG reported that the department did not have an effective information security program and has had deficient information security controls over its financial systems. The weaknesses described by the IG are consistent with the control deficiencies we identified during an examination of VA's high-impact systems[19] that we reported on in 2016.[20] In those reports, we described deficiencies in VA's implementation of access controls, patch management, and contingency planning. These deficiencies existed, in part, because the department had not effectively implemented key elements of its information security program. Until VA rectifies reported shortcomings in its agency-wide information security program, it will continue to have limited assurance that its sensitive information and information systems are sufficiently safeguarded.

[19]High-impact systems are those systems where the loss of confidentiality, integrity, or availability of the systems or the information they contain can have a severe or catastrophic adverse effect on an organization's operations, assets, or individuals. Such an impact can result in loss or degradation of mission capability, severe harm to individuals, or major financial loss.

[20]GAO-16-501 and GAO-16-691SU.

Adequately Mitigating Known Security Deficiencies

VA has not consistently mitigated known security deficiencies in a timely manner. As mentioned earlier, VA has reported a material weakness in information security for financial reporting purposes for 17 consecutive years. In fiscal year 2016, we recommended 74 actions for the department to take to improve its cybersecurity program and remedy known control deficiencies with selected high-impact systems.[21] However, as of October 2019, over 3 years later, VA had implemented only 32 (or 43 percent) of the 74 recommendations. One of the remaining unimplemented recommendations calls for the department to consistently and comprehensively perform security control assessments. This recommended activity is an important element of a cybersecurity program and helps to provide assurance that controls are operating as intended and to detect controls that are not functioning correctly.

VA has also been challenged in assuring that its actions to mitigate vulnerabilities and implement recommended improvements are effective. The department has asserted that it had implemented 39 of the 42 remaining open recommendations from our fiscal year 2016 reports. However, the evidence VA provided was insufficient to demonstrate that it had fully implemented the recommendations. The department subsequently provided additional evidence, which was also insufficient, indicating that its remedial action process was not validating the effectiveness of actions taken to resolve known deficiencies. Until VA adequately mitigates security control deficiencies, the sensitive data maintained on its systems will remain at increased risk of unauthorized modification and disclosure, and the systems will remain at risk of disruption.

Fully Establishing Elements of a Cybersecurity Risk Management Program

VA has been challenged in managing its cybersecurity risk. In July 2019, we reported that the department had fully met only one of the five foundational practices for establishing a cybersecurity risk management

[21]We issued five recommendations in the publicly available report, and an additional 69 recommendations in a separate report with limited distribution that we provided directly to VA. The accompanying report included recommendations to address weaknesses identified related to access control, patch management, and contingency planning. (GAO-16-501 and GAO-16-691SU respectively).

program.[22] Although VA established the role of a cybersecurity risk executive, the department had not fully:

- developed a cybersecurity risk management strategy that addressed key elements, such as risk tolerance and risk mitigation strategies;
- documented risk-based policies that required the department to perform agency-wide risk assessments;
- conducted an agency-wide cybersecurity risk assessment to identify, assess, and manage potential enterprise risks; or
- established coordination between cybersecurity and enterprise risk management.

VA concurred with our four recommendations to address these deficiencies and asserted that it is acting to do so. Nevertheless, until VA fully establishes a cybersecurity risk management program, its ability to convey acceptable limits regarding the selection and implementation of controls within the established organizational risk tolerance will be diminished.

Identifying Critical Cybersecurity Staffing Needs

VA has been challenged to accurately identify the work roles of its workforce positions that perform IT, cybersecurity, or cyber-related functions—a key step in identifying its critical cybersecurity staffing needs. In March 2019, we reported that the department had likely miscategorized the work roles of many of these positions in its personnel system.[23] Specifically, VA had reported that 3,008 (or 45 percent) of its 6,636 positions in the 2210 IT management occupational series—positions that most likely performed IT, cybersecurity, and cyber-related functions—were not performing these functions.[24]

VA concurred with our recommendation to review the work roles for positions in the 2210 IT management occupational series and assign the appropriate work roles, and stated that it had begun to do so.

[22]GAO-19-384.

[23]GAO-19-144.

[24]The 2210 IT management occupational series covers positions that manage, supervise, lead, administer, develop, deliver, and support information technology systems and services.

Nevertheless, until VA completely and accurately categorizes the work roles of its workforce positions performing IT, cybersecurity, and cyber-related functions, the reliability of the information needed to improve workforce planning will be diminished and its ability to effectively identify critical staffing needs will be impaired.

Managing IT Supply Chain Risks as Part of IT Modernization Programs

Assessing and managing supply chain risks are important considerations for agencies, including VA, when operating and modernizing IT systems. In July 2018, we reported that reliance on a global IT supply chain introduces risks to federal information systems.[25] We noted that supply chain threats are present during various phases of a system's development life cycle and we identified the following threats:

- Installation of malicious or intentionally harmful hardware or software;
- Installation of counterfeit hardware or software;
- Failure or disruption in the production or distribution of critical products;
- Reliance on a malicious or unqualified service provider; and
- Installation of hardware or software that contains unintentional vulnerabilities, such as defects in code that can be exploited.

These threats can have a range of impacts, including allowing adversaries to take control of systems or decreasing the availability of materials or services needed to develop systems.

Accordingly, agencies such as VA need to take appropriate measures to assess and manage IT supply chain risks as they operate and modernize their information systems. Failure to do so could result in data loss, modification, or exfiltration; loss of system availability; and a persistent negative impact on the agency's mission.

In summary, similar to other federal agencies, VA continues to be challenged in implementing an effective agency-wide program and controls for securing its information and information systems. As VA pursues efforts to modernize and secure its IT systems, it will need to

[25]GAO-18-667T.

successfully address multiple challenges in order to achieve effective outcomes.

Chair Lee, Ranking Member Banks, and Members of the Subcommittee, this completes my written statement. I would be pleased to answer your questions.

GAO Contact and Staff Acknowledgments

If you or your staff members have any questions concerning this testimony, please contact me at (202) 512-6244 or wilshuseng@gao.gov.

Contact points for our Office of Congressional Relations and Public Affairs may be found on the last page of this statement. Other individuals who made key contributions to this testimony include Jeffrey Knott (Assistant Director), Di'Mond Spencer (Analyst-in-Charge), Chris Businsky, Nancy Glover, Franklin Jackson, and Daniel Swartz. Also contributing were Melina Asencio, Scott Pettis, and Zsaroq Powe.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Phone

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

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

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

Connect with GAO

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

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

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

Congressional Relations

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

Public Affairs

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

Strategic Planning and External Liaison

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