U.S. GOVERNMENT ACCOUNTABILITY OFFICE

441 G St. N.W.
Washington, DC 20548

April 18, 2023

The Honorable Mark Takano
Ranking Member
Committee on Veterans' Affairs
House of Representatives

CYBERSECURITY: VA Needs to Address Privacy and Security Challenges

Accessible Version

Federal agencies, including the Department of Veterans Affairs (VA), collect and process large amounts of personally identifiable information (PII) that are used for various government programs.[1] The PII collected by federal agencies, along with the increasing sophistication of technology, highlights the importance of strong programs for ensuring privacy protections. Such programs are especially critical when considering recent breaches involving PII that have affected millions of people.[2]

Federal agencies, including VA, rely extensively on IT to carry out their operations and deliver services to constituents. Federal systems and networks, including those of VA, are often interconnected with other internal and external systems and networks, thereby increasing risk and the means used to initiate cyberattacks. Without proper safeguards, computer systems are vulnerable to individuals and groups with malicious intent who can intrude and use their access to obtain sensitive information, commit fraud and identity theft, disrupt operations, or launch attacks against other computer systems and networks. Since 1997, GAO has designated information security as a government-wide high-risk area—a designation that remains today.[3]

Health data, such as those managed by VA's electronic health record (EHR) system are essential to VA's ability to deliver health care services to about nine million veterans annually. In particular, the health care sector, including VA, uses a wide array of information systems and technologies across multiple settings, such as physician offices and hospitals. While the increasing use of health IT systems has the potential to improve health care quality, these systems can be vulnerable to the loss or unauthorized disclosure of patients' PII.

You asked us to review VA's privacy and security efforts. Specifically, we reviewed VA (1) privacy practices and challenges and (2) security challenges. To address both objectives, we reviewed prior reports and testimonies that described privacy and security challenges faced by

[1]In general, PII is any information that can be used to distinguish or trace an individual's identity, such as name, date or place of birth, and Social Security Number; or that otherwise can be linked to an individual.

[2]A breach is an unauthorized or unintentional exposure, disclosure, or loss of an organization's sensitive information.

[3]See GAO, *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas*, GAO-21-119SP (Washington, D.C.: Mar. 2, 2021); *High-Risk Series: An Overview*, GAO-HR-97-1 (Washington, D.C.: February 1997); and *High-Risk Series: Information Management and Technology*, GAO-HR-97-9 (Washington, D.C.: February 1997). In 2003, we expanded this area to include computerized systems supporting the nation's critical infrastructure and, in 2015, we further expanded this area to include protecting the privacy of personally identifiable information.

federal agencies, including VA.[4] In addition, we incorporated information on the department's actions in response to recommendations we made in our previous reports. More detailed information on our objectives, scope, and methodology for work can be found in the issued reports. We also reviewed relevant VA Office of Inspector General (OIG) reports on cybersecurity.[5]

We conducted this performance audit from November 2022 to April 2023 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

VA promotes the health, welfare, and dignity of all veterans in recognition of their service to the nation by ensuring that they receive benefits, social support, medical care, and lasting memorials. In carrying out this mission, the department operates one of the largest health care delivery systems in America, providing health care to millions of veterans and their families at more than 1,500 facilities.

To provide health care and other benefits to veterans and their dependents, VA relies on IT systems and networks to receive, process, and maintain sensitive data, including veterans' medical records and associated PII. VA maintains this information in a variety of systems, including in the Veterans Health Information Systems and Technology Architecture (VistA), its legacy EHR system.[6] For more than 30 years, VA has relied on VistA to provide EHR system capabilities and support the delivery of health care to veterans. The department has undertaken various attempts over the past two decades to modernize VistA, and we have previously reported on these efforts.[7]

---

[4]See, for example, GAO, *Privacy: Dedicated Leadership Can Improve Programs and Address Challenges*, GAO-22-105065 (Washington, D.C.: Sept. 22, 2022); *Cybersecurity: OMB Should Update Inspector General Reporting Guidance to Increase Rating Consistency and Precision*, GAO-22-104364 (Washington, D.C.: Mar. 31, 2022); *Electronic Health Records: VA Needs to Address Data Management Challenges for New System*, GAO-22-103718 (Washington, D.C.: Feb. 1, 2022); *Information Security: VA and Other Federal Agencies Need to Address Significant Challenges*, GAO-20-256T (Washington, D.C.: Nov. 14, 2019); and *Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges*, GAO-19-384 (Washington, D.C.: July 25, 2019).

[5]See, for example, Department of Veterans Affairs, Office of Inspector General, *Federal Information Security Modernization Act Audit for Fiscal Year 2021 (*Washington, D.C.: Apr. 13, 2022) and *Fiscal Year 2021 Inspector General's Report on VA's Major Management and Performance Challenges*.

[6]VistA supports a complex set of clinical and administrative capabilities and contains an EHR for each patient (i.e., a collection of information about the health of an individual or the care provided, such as patient demographics, progress notes, problems, medications, vital signs, past medical history, immunizations, laboratory data, and radiology reports). VistA has evolved into a technically complex system that supports health care delivery at more than 1,500 locations, including VA medical centers, outpatient clinics, community living centers, and VA vet centers. Customization of the system by local facilities has resulted in about 130 clinical versions of VistA—referred to as instances.

[7]See, for example, GAO-22-103718 and GAO, *Veterans Affairs: VA Needs to Address Persistent IT Modernization and Cybersecurity Challenges*, GAO-20-719T (Washington, D.C.: Sept. 16, 2020).

Implementing an effective information security program and controls is important for VA in protecting the sensitive health data and PII of veterans. In addition, vulnerabilities arising from VA's increased dependence on IT can result in the compromise of sensitive personal information, such as inappropriate use, modification, or disclosure. As a result, the corruption of data or the denial or delay of services for veterans due to compromised IT systems and electronic information can create undue hardship for veterans and their dependents.

Moreover, the federal government, including VA, continues to face challenges in protecting privacy and sensitive data. Information security incidents, many involving PII, continue to affect federal agencies and the privacy of U.S. citizens. For example, federal agencies reported 32,511 incidents to the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency in fiscal year (FY) 2021.

Federal Law and Policy Establish Requirements for Protecting PII and Securing Federal Systems and Information

Federal laws, along with executive branch guidance, establish agency requirements and responsibilities for ensuring the protection of PII and other sensitive personal information and ensuring privacy protections for agency programs.[8] These laws and guidance include:

- **Privacy Act of 1974.** The act places limitations on agencies' collection, disclosure, and use of personal information maintained in systems of records.[9]
- **E-Government Act of 2002.** The act requires that agencies conduct, where applicable, a privacy impact assessment (PIA) for each system.[10] This assessment is an analysis of how personal information is collected, stored, shared, and managed in a federal system.
- **Executive Order 13719, *Establishment of the Federal Privacy Council.*** This 2016 executive order established the Federal Privacy Council as the principal interagency forum to improve the government privacy practices of agencies and entities acting on their behalf. Further, it directed the Office of Management and Budget (OMB) to issue a revised policy on the role and designation of the senior agency officials for privacy (SAOP).[11]
- **OMB Memorandum M-16-24, *Role and Designation of Senior Agency Officials for Privacy.*** In September 2016, OMB issued guidance to clarify and update the role of the agency SAOP. It provides details on the SAOP's responsibilities. In particular, it states that

[8]This summary encompasses executive branch agencies generally. Individual agencies may also have responsibilities for overseeing privacy under area-specific privacy laws. For example, the Veterans Health Administration is a covered entity under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, title II, subtitle F, § 262(a), 110 Stat. 1936, 2021 (Aug. 21, 1996), and regulations including the HIPAA Privacy and Security Rule.

[9]Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (Dec. 31, 1974) (codified as amended at 5 U.S.C. § 552a). A system of records is a collection of information about an individual under control of an agency from which information is retrieved by the name of an individual or other identifier. 5. U.S.C. § 552a(a)(4), (5).

[10]E-Government Act of 2002, Pub. L. No. 107-347, § 208, 116 Stat. 2899, 2921-22 (Dec. 17, 2002).

[11]The White House, *Establishment of the Federal Privacy Council*, Executive Order 13719 (Washington, D.C.: Feb. 9, 2016).

the SAOP should have the skills, knowledge, and expertise to lead the agency's privacy program and the necessary authority to carry out privacy-related functions.[12]

In addition to laws and guidance focusing specifically on PII, agencies are subject to laws and guidance governing the protection of information and information systems, which includes implementing privacy protections. For example:

- **Federal Information Security Modernization Act of 2014 (FISMA).** The act requires each agency to develop, document, and implement an agency-wide information security program. FISMA requires agency Inspectors General to annually assess the effectiveness of the information security policies, procedures, and practices of their parent agency. Further, FISMA gives the National Institute of Standards and Technology (NIST) responsibility for developing standards for categorizing information and information systems, security requirements for information and systems, and guidelines for detection and handling of security incidents.[13]
- **NIST Special Publication 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations.** This document provides a catalog of security and privacy controls for systems and organizations.[14] While previous revisions of this publication included a separate appendix detailing specific privacy controls, revision 5, issued in September 2020, aims to fully integrate privacy controls into the security control catalog, creating a consolidated and unified set of controls.[15]

Federal Guidance Includes Key Practices for Establishing Privacy Programs

OMB and NIST guidance include key practices for establishing programs for ensuring privacy protections for agency programs.[16] Specifically, these include activities that lay the foundation for programs to develop and evaluate privacy policy, manage privacy risks, and ensure compliance with applicable privacy requirements. Based on this guidance, we previously reported on these 10 practices shown in table 1.[17]

[12]Office of Management and Budget, *Role and Designation of Senior Agency Officials for Privacy*, M-16-24 (Washington, D.C.: Sept. 15, 2016).

[13]The Federal Information Security Modernization Act of 2014 (FISMA 2014) Pub. L. No.113-283, 128 Stat. 3073 (Dec. 18, 2014) largely superseded the Federal Information Security Management Act of 2002 (FISMA 2002), enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this report, FISMA refers both to FISMA 2014 and to those provisions of FISMA 2002 that were either incorporated into FISMA 2014 or were unchanged and continue in full force and effect.

[14]National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, Special Publication 800-53, Revision 5 (Gaithersburg, MD: September 2020).

[15]Further, as a result of a major data breach, VA is subject to the Department of Veterans Affairs Information Security Act of 2006, title IX of Pub. L. No. 109-461 (120 Stat. at 3450), as amended, 38 U.S.C. §§ 5721-5728.

[16]This guidance includes: Office of Management and Budget, *Managing Information as a Strategic Resource,* OMB Circular A-130 (Washington, D.C.: July 2016); and National Institute of Standards and Technology, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, Special Publication 800-37, Revision 2 (Gaithersburg, MD: December 2018).

[17]GAO-22-105065.

Table 1: Ten Key Practices for Establishing a Program for Ensuring Privacy Protections

Category	Key practice	Description
Document privacy compliance activities	Develop system of records notices	Agencies are required to comply with the requirements of the Privacy Act of 1974 and ensure that system of records notices are published, revised, and rescinded, as required.
Document privacy compliance activities	Develop privacy impact assessments	Agencies are required to conduct privacy impact assessments in accordance with the E-Government Act of 2002.
Document privacy compliance activities	Develop and maintain a privacy program plan	Agencies are required to develop and maintain a privacy program plan that provides an overview of the agency's privacy program. The plan should also include the program management and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks.
Ensure coordination between privacy and other programs or functions	Coordination with information security program	Agencies should ensure that the senior agency official for privacy (SAOP) and the agency's privacy personnel closely coordinate specifically with agency officials responsible for information security.
Ensure coordination between privacy and other programs or functions	Coordination with IT budget and acquisition activities	The SAOP is responsible for reviewing IT capital investment plans and budgetary requests to ensure privacy requirements and associated controls are explicitly identified and included with respect to any IT resources that will involve personally identifiable information (PII).
Ensure coordination between privacy and other programs or functions	Coordination with workforce planning activities	The SAOP should be involved in assessing and addressing the hiring, training, and professional development needs of the agency with respect to privacy.
Ensure coordination between privacy and other programs or functions	Coordination with incident response activities	The SAOP should be notified of privacy-related incidents in accordance with procedures issued by the Office of Management and Budget.
Implement a risk management framework to manage privacy risks	Develop a privacy risk management strategy	Agencies should establish a risk management strategy for the organization that includes a determination of privacy risk tolerance.
Implement a risk management framework to manage privacy risks	Authorize information systems containing PII	Agencies should ensure the involvement of the SAOP or other privacy officials in the categorization, control selection, control assessment, and authorization of agency information systems with PII.
Implement a risk management framework to manage privacy risks	Develop a privacy continuous monitoring strategy	As part of an agency's risk management process, the appropriate privacy official is to develop and maintain a written strategy for monitoring privacy controls on an ongoing basis.

Source: GAO analysis of Office of Management and Budget and National Institute of Standards and Technology guidance. | GAO-23-106412

VA Implemented Some but Not All Key Practices for Ensuring Privacy Protections

In September 2022, we reported that the 24 agencies addressed in the Chief Financial Officers (CFO) Act of 1990[18] varied in the extent to which they established policies and procedures and

[18]The CFO Act, Pub. L. No. 101-576, 104 Stat. 2838 (Nov. 15, 1990), as amended, established chief financial officers to oversee financial management activities at 23 civilian executive departments and agencies as well as the Department of Defense. The list of 24 entities is often referred to collectively as CFO Act agencies, and is codified, as amended, in Section 901(b) of Title 31 of the U.S. Code. The 24 agencies are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the

implemented key practices for ensuring privacy protections.[19] Among our recommendations, we made four to VA to fully address these practices in their privacy policies and procedures.

Specifically, our September 2022 report highlighted the extent to which VA addressed 10 practices for implementing its privacy programs. For six of the 10 practices, VA had

- established policies and procedures for developing system of records notices to identify personal data collected and how they are used;
- established policies and procedures for conducting privacy impact assessments;
- documented a privacy program plan;
- ensured that SAOP and other privacy personnel coordinate with the department's staff responsible for information security activities;
- defined roles and responsibilities for the SAOP and other privacy officials with respect to responding to privacy incidents including breaches of PII; and
- developed a privacy risk management strategic plan, which discussed the department's privacy risk tolerance.

The department had not fully implemented four of the selected practices. VA subsequently implemented one of the four practices.

- **Coordinate with IT budget and acquisition activities.** VA partially defined and documented a process for the involvement of privacy officials in reviewing budget requests. We recommended that VA establish a process for ensuring that the senior agency official for privacy, or other designated privacy official, reviews IT capital investment plans and budgetary requests, and document this process. VA concurred with our recommendation but, as of February 2023, VA had not yet fully implemented it. Until it does so, VA lacks assurance that privacy requirements and associated controls are explicitly identified and included with respect to any IT resources that will involve PII.
- **Coordinate with workforce planning activities.** VA had not fully defined or documented processes for privacy workforce management. For example, VA described processes for workforce planning but did not provide documentation of the role of the SAOP or other privacy officials in those processes. We recommended that VA fully define and document a process for ensuring that the SAOP, or other designated privacy official, is involved in assessing and addressing the hiring, training, and professional development needs of the agency with respect to privacy. VA concurred with our recommendation but, as of February 2023, VA had not yet fully implemented it. Implementing our recommendation by involving the SAOP or other privacy officials can benefit VA in its ability to identify staffing needs and ensure a well-qualified workforce.
- **Authorize information systems containing PII.** VA partially defined and documented the role of privacy officials in carrying out risk management steps for authorizing information systems with PII. In particular, VA noted that it had processes in place for involving privacy officials in each step, but the involvement of privacy officials was not always documented in the department's policies and procedures. We recommended that VA fully define and document the role of the SAOP, or other designated privacy official, in reviewing and approving system categorizations, overseeing privacy control assessments, and reviewing

Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Personnel Management; Small Business Administration; Social Security Administration; and U.S. Agency for International Development.

[19]GAO-22-105065.

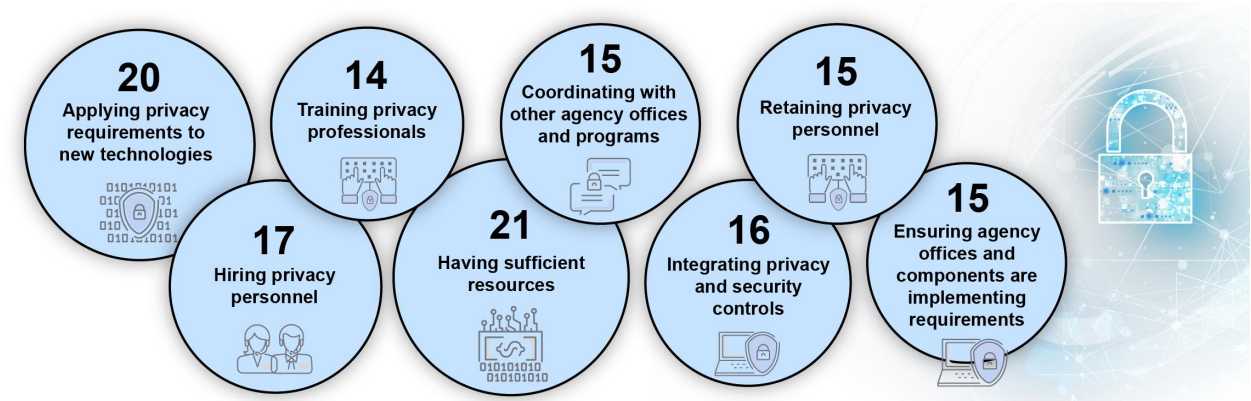
authorization packages. VA concurred with our recommendation but, as of February 2023, VA had not yet fully implemented it. Until VA implements the recommendation, the department's privacy program lacks assurance that privacy protections are adequately incorporated into those systems with PII.

- **Develop a privacy continuous monitoring strategy.** VA had not fully developed a continuous monitoring strategy. In particular, while VA had established a strategy, it had not included all elements, such as cataloging its privacy controls. We recommended that VA ensure that its privacy continuous monitoring strategy included a catalog of privacy controls and defined the frequency at which they are to be assessed. VA concurred with our recommendation and implemented it in October 2022.

Challenges in Implementing Privacy Programs

Privacy officials reported experiencing challenges in implementing their privacy programs.[20] Figure 1 shows the challenges most frequently identified and the number of agencies reporting each challenge. VA identified each of these challenges as ones facing its department's privacy program.

Figure 1: Number of 24 Chief Financial Officers Act of 1990 Agencies Reporting Challenges in Implementing Privacy Programs



Source: GAO analysis of agency survey responses; images: Thitichaya/stock.adobe.com, marinashevchenko/stock.adobe.com. | GAO-23-106412

VA Has Faced Challenges in Securing Its Information Systems

Coordination with the information security program is an important practice for ensuring privacy protection. This includes taking a coordinated approach to identifying and managing privacy and security risks and complying with applicable requirements. VA OIG and GAO have highlighted security challenges that VA has faced in safeguarding its information and information systems.[21] Specifically, VA OIG's FY 2021 FISMA report noted that VA faced challenges implementing

[20]GAO-22-105065.

[21]See, for example, GAO-22-104364; GAO-20-719T; GAO-19-384; GAO, *Information Security: Agencies Need to Improve Implementation of Federal Approach to Security Systems and Protecting against Intrusions*, GAO-19-105 (Washington, D.C.: Dec. 18, 2018); *Information Security: Agencies Need to Improve Controls over Selected High-Impact Systems*, GAO-16-501 (Washington, D.C.: May 18, 2016); *Information Security: VA Needs to Improve Controls over Selected High-Impact Systems*, GAO-16-691SU (Washington, D.C.: Sept. 30, 2016); and Department of Veterans Affairs, Office of Inspector General, *Fiscal Year 2021 Inspector General's Report on VA's Major Management and Performance Challenges*.

components of its agency-wide information security program to meet FISMA requirements.[22] The report identified continuing significant deficiencies related to access controls, configuration management controls, change management controls, and service continuity practices designed to protect mission-critical systems from unauthorized access, alteration, or destruction. The report included 26 recommendations for improving VA's information security program. VA concurred with 21, partially concurred with three, and did not concur with two recommendations. In addition, an OMB report to Congress summarizing FY 2021 agency cybersecurity performance noted that an independent assessment had concluded that VA's program was not effective.[23]

Further, in July 2019, we reported that the department had fully met one of the five foundational practices for establishing a cybersecurity risk management program by establishing a Cybersecurity Risk Executive.[24] However, VA did not meet four other cybersecurity practices. For example, VA did not (1) include key elements in its cybersecurity risk management strategy, (2) have a policy for an agency-wide risk assessment, (3) implement a process to identify enterprise cybersecurity risks, and (4) establish coordination between its cybersecurity risk executive and enterprise risk management functions. We made four recommendations, and the department has since implemented them all.[25] Nevertheless, continued attention to these security challenges is important. The provision of timely and quality health care and benefits for veterans and other eligible individuals depends, in large part, on the security functionality and effectiveness, as well as the ease of use of VA's information systems.

Agency Comments

We provided a draft of this report to VA for review and comment. The department's audit liaison provided technical comments via email. We incorporated these comments as appropriate.

We are sending copies of this report to the appropriate congressional committees, the Secretary of Veterans Affairs, and other interested parties. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

[22]Department of Veterans Affairs, Office of Inspector General, *Federal Information Security Modernization Act Audit for Fiscal Year 2021 (*Washington, D.C.: Apr. 13, 2022).

[23]Office of Management and Budget, *Federal Information Security Modernization Act of 2014 Annual Report to Congress, Fiscal Year 2021* (Washington, D.C.: Sept. 14, 2022). This report provided summaries of agency-specific cybersecurity performance narratives, which included, among other things, independent assessments of agency-specific information security programs.

[24]GAO-19-384.

[25]We also made 74 recommendations for the department to take to improve its cybersecurity program and remedy control deficiencies in GAO-16-691SU and GAO-16-501. VA has taken actions to address 73 of these recommendations. VA did not implement the remaining recommendation due to technical constraints.

If you or your staff have any questions about this report, please contact me at (404) 679-1831 or franksj@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report included Tammi Kalugdan and Jeffrey Knott (Assistant Directors), Amanda Andrade, Mark Bird, Chris Businsky, Donna Epler, Shane Homick, Lee McCracken, Scott Pettis, Kevin Smith, Umesh Thakkar (analyst-in-charge), and Alec Yohn.

Jennifer R. Franks
Director, Center for Enhanced Cybersecurity
Information Technology and Cybersecurity