United States Government Accountability Office

Report to Chair, Subcommittee on Emerging Threats and Spending Oversight, Committee on Homeland Security and Governmental Affairs, U.S. Senate

December 2021

DHS PRIVACY

Selected Component Agencies Generally Provided Oversight of Contractors, but Further Actions Are Needed to Address Gaps

Accessible Version

GAO@100
A Century of Non-Partisan Fact-Based Work

GAO-22-104144

GAO Highlights

Highlights of GAO-22-104144, a report to Chair, Subcommittee on Emerging Threats and Spending Oversight, Committee on Homeland Security and Governmental Affairs, U.S. Senate

December 2021

DHS PRIVACY

Selected Component Agencies Generally Provided Oversight of Contractors, but Further Actions Are Needed to Address Gaps

Why GAO Did This Study

It is essential that DHS, its component agencies, and its contractors protect the PII that they collect and maintain. Implementing and enforcing appropriate policies and controls can help prevent improper PII access and use.

GAO was asked to review DHS's policies and procedures for protecting the PII collected by or shared with its contractors. This report discusses the extent to which (1) DHS has developed policies and procedures to mitigate the risks to PII; (2) selected DHS components have provided oversight of privacy controls within contractor-operated systems, and (3) DHS components have ensured that privacy incidents in contractor-operated systems are properly identified and remediated.

GAO analyzed DHS policies and procedures, selected and reviewed six major DHS components, evaluated contractor-operated system documentation related to the oversight of privacy controls, and compared contractor-related privacy incident handling and response activities to DHS requirements. GAO also interviewed relevant officials at DHS and its major components.

What GAO Recommends

GAO is making seven recommendations to DHS components to improve their oversight of contractors' privacy controls and remediation of incidents. DHS concurred with the recommendations and outlined steps planned or taken to address them.

View GAO-22-104144. For more information, contact Nick Marinos at (202) 512-9342 or marinosn@gao.gov.

What GAO Found

The Department of Homeland Security (DHS) developed policies and procedures to mitigate the risks to personally identifiable information (PII) on contractor-operated IT systems. These policies address federal privacy requirements, standards, and guidelines in the following key areas:

- Establishing and maintaining a comprehensive privacy program.
- Providing agency-wide privacy training for all employees and contractors.
- Overseeing information systems operated by contractors.
- Ensuring implementation of privacy controls for contractor systems.
- Ensuring incident response procedures for contractor systems.

As shown below, selected DHS components addressed most of the key privacy control activities for overseeing contractor-operated systems.

Assessment of Selected DHS Components' Oversight of the Implementation of Privacy Controls in Selected Contractor-Operated Systems

Associated activities	CBP	DHS HQ	FEMA	ICE	TSA	USCG
Establish roles and responsibilities	Met	Met	Met	Met	Met	Met
Define privacy requirements in contracts	Met	Met	Met	Met	Met	Met
Identify and address gaps in privacy compliance	Met	Met	Met	Met	Met	Not met
Develop and implement a comprehensive training policy	Met	Met	Met	Met	Met	Met
Administer annual privacy training and targeted role-based privacy training	Met	Partially met	Met	Met	Met	Partially met
Establish and maintain an inventory of all programs and systems with PII	Met	Met	Met	Met	Met	Met
Provide information to contractors describing PII in their possession	Met	Met	Met	Met	Met	Met
Evaluate any proposed new instances of sharing PII with third parties	Met	Met	Met	Met	Not met	Not met

CBP = U.S. Customs and Border Protection, DHS HQ = Department of Homeland Security headquarters, FEMA = Federal Emergency Management Agency, ICE = Immigration and Customs Enforcement, TSA = Transportation Security Administration, USCG = United States Coast Guard

Met = met associated activities; partially met = partially met associated activities; not met = did not meet associated activities

Source: GAO analysis of agency-provided data.| GAO-22-104144

Although the DHS components complied with most of the requirements, gaps existed. For example, USCG did not demonstrate that it identified and addressed gaps in privacy compliance, DHS HQ did not administer role-based privacy training, and TSA did not demonstrate its evaluation of proposed new instances of PII sharing in contractor-operated systems.

Regarding privacy incidents, DHS developed *Privacy Incident Handling Guidance*, which outlines the department's process for how incidents are to be identified and remediated. Of the four reviewed components that had a breach of data, three fully identified, remediated, and shared lessons learned for the incidents. However, one component did not document all necessary remediation activities. Fully documenting remediation activities helps ensure that all appropriate steps have been taken to lessen potential harm that the loss, compromise, or misuse of PII could have on affected individuals.

Contents

GAO Highlights 2

Why GAO Did This Study 2
What GAO Recommends 2
What GAO Found 2

Letter 1

Background 4
DHS Has Developed Policies and Procedures to Ensure the Privacy of PII in Contractor-Operated Systems 12
Components Followed Oversight Requirements for Privacy Controls in Contractor-Operated Systems, but Some Controls Were Not Fully Implemented 17
Most DHS Components Implemented Procedures to Identify, Remediate, and Share Lessons Learned 23
Conclusions 29
Recommendations for Executive Action 29
Agency Comments and Our Evaluation 30

Appendix I: Objectives, Scope, and Methodology 33

Appendix II: Comments from the Department of Homeland Security 38

Text of Appendix II: Comments from the Department of Homeland Security 43

Appendix III: GAO Contact and Staff Acknowledgments 48

GAO Contact 48
Staff Acknowledgments 48

Tables

Assessment of Selected DHS Components' Oversight of the Implementation of Privacy Controls in Selected Contractor-Operated Systems 2
Data table for Figure 1: Privacy Incidents Reported to Congress by the Department of Homeland Security (DHS), 2015 through 2019 5
Table 1: Department of Homeland Security (DHS) Oversight Activities Required for the Implementation of Privacy Controls in Contractor-Operated Systems 17

Table 2: Assessment of Selected Department of Homeland Security (DHS) Components' Oversight of the Implementation of Privacy Controls in Selected Contractor-Operated Systems 18

Figure

Figure 1: Privacy Incidents Reported to Congress by the Department of Homeland Security (DHS), 2015 through 2019 5

Abbreviations

CBP	U.S. Customs and Border Protection
DHS	Department of Homeland Security
DHS HQ	Department of Homeland Security headquarters
FAR	Federal Acquisition Regulation
FEMA	Federal Emergency Management Agency
FISMA	*Federal Information Security Modernization Act of 2014*
ICE	U.S. Immigration and Customs Enforcement
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PIA	privacy impact assessment
PIHG	*Privacy Incident Handling Guidance*
PII	personally identifiable information
PTA	privacy threshold analysis
SORN	system of records notice
TSA	Transportation Security Administration
USCG	U.S. Coast Guard

GAO@100 U.S. GOVERNMENT ACCOUNTABILITY OFFICE
A Century of Non-Partisan Fact-Based Work

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

December 16, 2021

The Honorable Margaret Wood Hassan
Chair
Subcommittee on Emerging Threats and Spending Oversight
Committee on Homeland Security and Governmental Affairs
United States Senate

Dear Madam Chair:

The Department of Homeland Security (DHS) is responsible for a wide variety of functions that are critically important to maintaining the security of our nation's citizens. To carry out these functions, the department needs to collect and maintain extensive amounts of detailed and sometimes sensitive personally identifiable information (PII). The types of PII can include a person's name, date, place of birth, Social Security number, or other types of personal information that can be linked to an individual, such as medical, educational, financial, and employment information.

In many cases, DHS leverages the capabilities and expertise of contractors to assist in its various missions and grants contractor employees access to PII in order to perform the work. It is essential that the PII collected and maintained on the department's behalf on contractor-operated IT systems not be disclosed inappropriately. Federal laws and guidance require DHS and component agencies to have strong policies and procedures in place and to use them to guide their protection of information, particularly of PII.

You asked us to review DHS's policies and procedures for ensuring that the PII collected by or shared with contractors is protected from improper access or use. Our specific objectives were to examine the (1) extent to which DHS has developed policies and procedures for the protection of PII that is collected, used, or stored by contractors; (2) extent to which selected major DHS components oversee the implementation of privacy controls within contractor-operated systems that collect, use, or store PII on behalf of the department; and (3) actions DHS has taken to ensure that privacy incidents that occur in contractor-operated systems at the component level are identified and remediated in an effective and timely manner and that lessons learned are shared with all components, as appropriate.

To address the first objective, we analyzed DHS policies, procedures, and other documentation that describe the department's requirements to protect PII that is collected, used, or stored by contractors. We then compared them to selected privacy requirements specified in relevant federal laws and Office of Management and Budget (OMB) and National Institute of Standards and Technology (NIST) guidance.[1]

In selecting the practices for our assessment, we focused on those practices identified by federal laws and OMB and NIST guidance that addressed the oversight of contractors that collect, use, or store information on behalf of a government entity. Based on these criteria, we selected five practices on establishing a comprehensive privacy program, conducting privacy training, overseeing privacy in information systems operated by contractors, ensure implementation of privacy controls, and ensuring that privacy incident response procedures are in place for contractor information systems. We also conducted interviews with officials from the DHS Privacy Office to gain insight into how their policies and procedures addressed the practices aimed at protecting PII that is accessible by contractors.

For the second and third objectives, we reviewed six DHS components' efforts to oversee privacy-related issues within contractor-operated systems that collect, use, or store PII on behalf of the department.[2] To select the major DHS components to be included in our review, we

[1]The federal laws and guidance we reviewed to determine the selected data protection requirements included: (1) the *Privacy Act of 1974*; (2) the *E-Government Act of 2002*; (3) the *Federal Information Security Modernization Act of 2014*; (4) the *Federal Acquisition Regulation* Subpart 24.1; (5) the *Homeland Security Acquisition Regulation*, 48 C.F.R. Subpart 3024.1; (6) Office of Management and Budget (OMB) *Managing Information as a Strategic Resource*, Circular A-130; (7) OMB, *Preparing for and Responding to a Breach of Personally Identifiable Information*, M-17-12; (8) National Institute of Standards and Technology (NIST), *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53 Rev. 4*;* (9) NIST, *Risk Management Framework for Information Systems and Organizations*, Special Publication 800-37 Rev.2.

[2]The major operational components that currently make up the Department of Homeland Security are: U.S. Citizenship and Immigration Services, U.S. Coast Guard, U.S. Customs and Border Protection, Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security Headquarters, Federal Emergency Management Agency, Federal Law Enforcement Training Center, U.S. Immigration and Customs Enforcement, U.S. Secret Service, and Transportation Security Administration.

requested a list of privacy incidents[3] that occurred in DHS major components' contractor-operated systems within the time period of July 1, 2018 to June 30, 2019. From the data DHS provided, we determined that six major components had experienced a privacy incident: U.S. Coast Guard (USCG), U.S. Customs and Border Protection (CBP), U.S. Department of Homeland Security Headquarters (DHS HQ), Federal Emergency Management Agency (FEMA), U.S. Immigration and Customs Enforcement (ICE), and Transportation Security Administration (TSA).

For the second objective, we reviewed relevant documentation pertaining to specific contractor-operated systems at each of the six selected components we selected for review and compared the information to DHS requirements related to the oversight of privacy controls within those systems. To identify the contractor-operated systems included in our review, we selected from each of the six components the system that had experienced the highest reported risk level privacy incident from July 01, 2018 through June 30, 2019.

In order to identify the DHS requirements to include in our review, we considered those requirements in DHS's *Sensitive Systems Handbook* and acquisition policies that are focused on areas related to the oversight of contractor implementation of privacy controls. We also interviewed relevant agency officials, such as the DHS Chief Privacy Officer, component-level security and privacy officials, and relevant contractor staff, to discuss the oversight of privacy controls in the selected contractor-operated systems.

To address the third objective, we selected four of the six major components to include in our review because they had privacy incidents that resulted in a data breach. Of those four major components, we reviewed documentation on specific contractor-related privacy incidents that occurred at the components and compared the documentation to selected DHS requirements related to privacy incident handling and response.

[3]DHS defines a "privacy incident" as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than the authorized user accesses or potentially accesses [PII] or (2) an authorized user accesses or potentially accesses [PII] for an unauthorized purpose. The term encompasses both suspected and confirmed incidents involving PII, whether intentional or inadvertent, which raises a reasonable risk of harm.

To identify the privacy incidents included in our review, we selected the incident with the highest reported risk level within each component during the requested time frame. In those instances where there were multiple incidents reported at the highest risk level within a component, we selected the most recent incident.

To identify DHS privacy incident handling requirements, we reviewed requirements specified in DHS's *Privacy Incident Handling Guidance* (PIHG)[4] and focused on requirements related to identifying and remediating privacy incidents and sharing lessons learned with other components. We also interviewed relevant agency officials, such as component privacy and information security and contractor staff, to gain additional insight into the steps they took to identify and remediate the specific incidents. Additionally, we inquired about steps they took to share lessons learned with other components. A more complete description of our objectives, scope, and methodology is provided in appendix I.

We conducted this performance audit from March 2020 to December 2021 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Federal agencies use information systems and electronic data to carry out their missions. Protecting these systems and the information that resides on them, which can include PII, is essential to prevent unauthorized or unintentional exposure, disclosure, or loss that can lead to serious consequences and result in substantial harm to individuals and the federal government. Specifically, ineffective protection of IT systems and information can result in

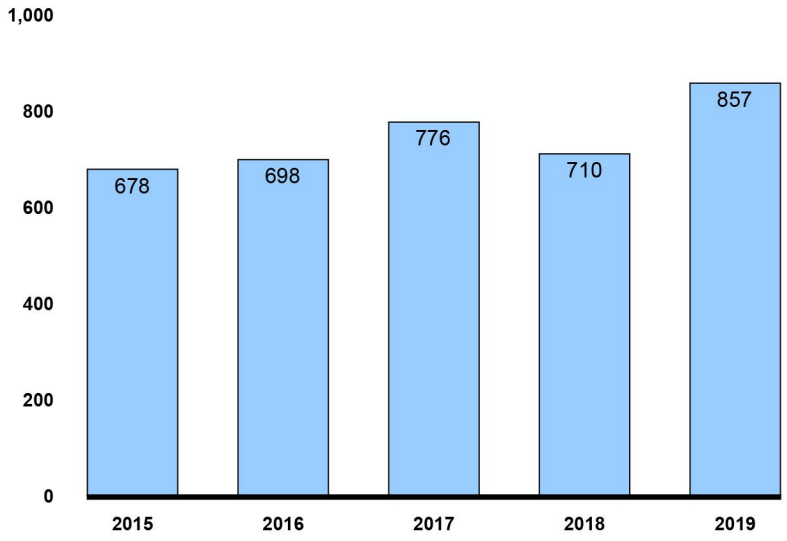
- inappropriate access to and disclosure, modification, or destruction of sensitive information;
- loss or theft of resources, including money and intellectual property;

[4]Department of Homeland Security Privacy Office, *Privacy Incident Handling Guidance*, 047-01-008 (Washington, DC: Dec. 4, 2017).

- loss of privacy, emotional distress, or reputational harm;
- loss of public confidence; or
- high costs to remediate the effects of a breach.

Federal agencies, including DHS, have reported increasing numbers of privacy incidents that have placed sensitive information at risk, with potentially serious impacts on federal operations, assets, and people. Figure 1 shows the number of privacy incidents DHS's Privacy Office reported to Congress annually, from 2015 through 2019.

Figure 1: Privacy Incidents Reported to Congress by the Department of Homeland Security (DHS), 2015 through 2019



Source: GAO analysis of DHS provided data. | GAO-22-104144

Data table for Figure 1: Privacy Incidents Reported to Congress by the Department of Homeland Security (DHS), 2015 through 2019

Year	Number of Incidents
2015	678
2016	698
2017	776
2018	710
2019	857

Source: GAO analysis of DHS provided data. | GAO-22-104144

DHS Relies on Contractors to Operate Its Information Systems

DHS has various missions, such as preventing terrorism, managing U.S. borders, and the security of cyberspace. To accomplish its broad and complex missions, the department has approximately 240,000 personnel (both employees and contractors). The department relies on IT and telecommunications to carry out its functions. In fiscal year 2020, the department obligated approximately $7.6 billion in total IT spending.

Contractors and their employees provide services to, and operate systems for, federal agencies at agency and contractor facilities. Services provided by contractors can include computer and telecommunications systems and services, testing, quality control, installation, and operation of computer equipment.

While contractor personnel who operate systems and provide services to federal agencies can provide significant benefits, they can also introduce risks to agency information and systems, such as the unauthorized access, use, disclosure, and modification of federal data. Specifically, contractor employees who have access to agency data and technology can introduce risks that can degrade or diminish the privacy of agency data or systems.

Contractors and contractor employees have been involved in DHS privacy incidents that included the unauthorized disclosure of federal information. For example,

- In March 2019, the DHS Office of Inspector General announced that FEMA's Transitional Sheltering Assistance program had overshared PII, such as banking and home address information, from more than 2.3 million survivors of hurricanes Harvey, Irma, and Maria, as well as California wildfires, with one of the agency's contractors. The DHS Office of Inspector General noted that the oversharing of PII increased the risk of identity theft and fraud.
- According to the DHS Office of Inspector General's September 2020 report, photographs of people in vehicles entering and exiting the U.S. through a land border port of entry had been stolen by hackers as part of a malicious cyberattack on one of CBP's subcontractor's private

networks.[5] This attack compromised approximately 100,000 images of travelers and at least 19 of the images had been posted to the dark web. The report noted that this incident may have damaged the public's trust in the government's ability to safeguard biometric data and may have resulted in travelers' reluctance to permit DHS to capture and use their biometrics at U.S. ports of entry.

Federal Laws, Regulations, and Guidance Provide a Framework for Protecting the Privacy of Data and Information Systems

Federal laws require agencies to protect the privacy of federal data and information systems. Specifically, the *Privacy Act of 1974* limits how federal agencies collect, disclose, or use personal information.[6] Under this act, agencies are to, among other things, establish appropriate safeguards to ensure the security and confidentiality of personal information maintained in a system of records and protect it against anticipated security or integrity threats or hazards.[7] *Privacy Act* requirements also apply to government contractors and contractor personnel who have access to, or maintain, agency systems of records that contain PII.[8]

In addition, the *E-Government Act of 2002* addresses the protection of personal information in government information systems or information collections by requiring that agencies conduct a privacy impact assessment (PIA)—an analysis of how personal information is collected, stored, shared, and managed in a federal system.[9] The assessment helps

[5]DHS, Office of Inspector General, *Review of CBP's Major Cybersecurity Incident During a 2019 Biometric Pilot, OIG-20-71* (Washington, DC: Sept. 21, 2020).

[6]5 U.S.C. § 552a.

[7]A system of records is a collection of information about individuals under control of an agency from which information is retrieved by the name of an individual or other identifier.

[8]The *Privacy Act* requires that agencies notify the public through a system-of-records notice in the *Federal Register* that includes the policies and practices of the agency regarding storage, retrievability, and access controls when the agency establishes or makes changes to a system of records. The *Privacy Act* also requires that agencies establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records.

[9]Pub. L. No. 107-347, § 208, 116 Stat. 2899, 2921 (Dec. 17, 2002); 44 U.S.C. § 3501 note.

inform the selection of controls that are intended to protect a system, including contractor-operated systems. Among other requirements, an agency must conduct a PIA before developing or procuring IT that collects, maintains, or disseminates information that is in a personally identifiable form. In conducting a PIA, an agency must ensure that the handling of the information conforms to applicable privacy legal requirements, determine the risks, and examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[10]

The *Federal Information Security Modernization Act of 2014* (FISMA), addresses the protection of PII in the context of securing agency information and information systems.[11] FISMA and implementing policies and guidance from OMB and NIST, require agencies to ensure the adequate protection of agency information, including information collected or maintained by a contractor, as well as information systems operated by a contractor on behalf of an agency.[12]

For example, OMB has issued guidance to federal agencies on how to prepare for and respond to privacy incidents. Specifically, the guidance reiterates agency responsibilities under FISMA and technical guidance developed by NIST, drawing particular attention to requirements for protecting PII.[13] Also, OMB's Circular A-130 establishes general policy for the planning and management of federal information that includes the management of PII. Specifically, the circular requires agencies to

[10]Office of Management and Budget, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, M-03-22 (Sept. 26, 2003).

[11]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 report, FISMA refers to the new requirements in FISMA 2014, and to other relevant FISMA 2002 requirements that were unchanged by FISMA 2014 and continue in full force and effect.

[12]The National Institute of Standards and Technology (NIST) provides technical leadership for the nation's measurement and standards infrastructure, including the development of management, administrative, technical, and physical standards for the security of information in federal information systems. NIST's 800-series of special publications focuses on research, guidelines, and outreach efforts in information system security.

[13]Office of Management and Budget, *Preparing for and Responding to a Breach of Personally Identifiable Information*, M-17-12 (Washington, D.C.: Jan. 3, 2017).

develop, implement, document, maintain, and oversee agency-wide privacy programs.[14]

NIST has responsibilities for developing standards for categorizing information and information systems according to ranges of risk levels. It also has developed guidelines for detecting and handling information security incidents, including those involving PII. In particular, NIST Special Publications 800-53 and 800-53A guide agencies in selecting privacy controls for systems and assessing them to ensure that the selected controls are in place and functioning as expected.[15] Additional NIST special publications on IT security services and risk management (Special Publications 800-35 and 800-37) identify several activities important to contractor oversight for assessing the privacy controls of information systems.[16]

The *Federal Acquisition Regulation* (FAR) is the primary regulation that provides uniform policies and procedures for acquisitions by executive agencies.[17] The FAR requires agencies to address security considerations in acquisition planning, including a discussion of how agency information security requirements will be met. Also, for acquisitions requiring routine contractor access, a discussion is to be included of agency requirements for personal identity verification of contractors.

In addition, according to the FAR, acquisition planning processes should address basic safeguarding of information systems operated by contractors on behalf of the government. Further, the FAR requires the insertion of clauses into contracts implementing requirements prescribed

[14]Office of Management and Budget, *Managing Information as a Strategic Resource*, OMB Circular A-130 (July 28, 2016).

[15]National Institute of Standards and Technology (NIST), *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53 Rev. 4 (Gaithersburg, MD: April 2013). NIST 800-53 Revision 5 replaced Revision 4, but the September 23, 2021, implementation deadline had not yet arrived when we completed our analysis. Revision 4 was relevant during our reporting period and used as criteria.

[16]National Institute of Standards and Technology (NIST), *Guide to Information Technology Security* Services, Special Publication 800-35 (Gaithersburg, MD: Oct. 2003) and NIST, *Risk Management Framework for Information Systems and Organizations*, Special Publication 800-37 Rev.2 (Gaithersburg, MD: Dec. 2018) and

[17]The *Federal Acquisition Regulation* (FAR) contains the rules, standards, and requirements for the award, administration, and termination of government contracts.

in statute or executive order for contractor protection of certain categories of sensitive information, such as information related to the privacy of individuals.

DHS Privacy Office and Component Agencies' Responsibilities

The DHS Privacy Office is led by the Chief Privacy Officer, a position created by the *Homeland Security Act of 2002*.[18] The Chief Privacy Officer serves as the principal advisor to the DHS Secretary regarding privacy protections and the transparency of government operations for DHS. All DHS IT systems, technologies, rulemakings, programs, pilot projects, information collections, information sharing activities, or forms that collect PII or have a privacy impact are subject to the oversight of the Chief Privacy Officer. The Privacy Office is responsible for ensuring that technologies used at the department sustain privacy protections related to the use, collection, and disclosure of personal information. The office is also responsible for overseeing every DHS program and component to ensure that privacy considerations are addressed when planning or updating any program, system, or initiative.

In addition, the DHS Privacy Office is tasked with implementing the department's *Fair Information Practice Principles*, which govern the use of PII through a privacy compliance process.[19] Among other things, the office is to:

- Work with every DHS component and program in the department to ensure privacy considerations are addressed when planning or updating any program, system, form, or initiative that might use PII.

[18]6 U.S.C. § 142. Privacy officer.

[19]The *Fair Information Practice Principles*, which informed the *Privacy Act* requirements, are a set of principles for protecting the privacy and security of personal information that were first proposed in 1973 by a U.S. government advisory committee. These principles were intended to address what the committee considered the poor level of protection then being afforded to privacy under contemporary law. Since that time, the *Fair Information Practice Principles* have been widely adopted as a benchmark for evaluating the adequacy of privacy protections. The principles used for privacy policy and implementation at DHS are Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability and Auditing.

- Evaluate legislative and regulatory proposals involving the collection, use, and disclosure of PII.
- Centralize programmatic oversight of the *Freedom of Information Act*[20] and *Privacy Act* operations and supports implementation across the department.
- Operate a department-wide privacy incident response program to ensure incidents involving PII are properly reported, investigated, and mitigated, as appropriate.
- Respond to complaints of privacy violations and provides redress, as appropriate.
- Provide training, education, and outreach to build a culture of privacy across the department and transparency to the public.

The Privacy Office also is expected to work with the component agencies to ensure that all DHS systems, technology, forms, and programs that collect PII incorporate privacy protections. Each component is required to have either a privacy officer or a privacy point of contact. To ensure consistent communication, the Privacy Office is expected to coordinate monthly privacy compliance meetings and assigns a staff that serves as a liaison to each component agency in the event that privacy issues arise.

In addition, according to the department's privacy guidance, component agencies can develop additional privacy policies, as needed, to address specific mission roles or programs of the component agencies. These policies must be consistent with DHS Privacy Office policies and guidance to ensure consistency in privacy policy across the department and consistency with the *Fair Information Practice Principles*.

[20]5 U.S.C. § 552.

DHS Has Developed Policies and Procedures to Ensure the Privacy of PII in Contractor-Operated Systems

To ensure that contractor-operated systems meet federal privacy requirements [21] the FAR[22] requires that agency acquisition planning for IT comply with the privacy requirements in FISMA;[23] OMB's implementing policies,[24] including appendix III of OMB Circular A-130; and NIST guidance and standards. In reviewing these documents, we identified the following key requirements:

- establish and maintain a comprehensive privacy program that ensures compliance with applicable privacy requirements and develops and evaluates privacy policy;
- maintain and implement mandatory agency-wide privacy training for all employees and contractors;
- oversee privacy in information systems operated by contractors on behalf of the federal government that collect or maintain federal information;
- ensure the privacy controls implemented within information systems that are used by contractors on behalf of the agency comply with NIST standards and guidelines and agency requirements; and
- ensure that incident response procedures are in place for contractor information systems that operate on behalf of the agency, including

[21]*Privacy Act of 1974*, 5 U.S.C. § 552a; *E-Government Act of 2002*, Pub. L. No. 107-347, § 208, 116 Stat. 2899 (Dec. 17, 2002).

[22]The FAR establishes uniform policies and procedures for the acquisition of supplies and services by executive agencies. The FAR and the agency supplements are codified in title 48 of the *Code of Federal Regulations*. As relevant here, the FAR's requirements for acquisitions of information technology are at 48 C.F.R. Part 39. The acquisition planning requirements for IT security are at 48 C.F.R. § 7.103(w). See also, FAR § 7.105(b)(16)(*Government-furnished information*) and (18)(*Security considerations*). FAR Subpart 24.1 addresses protection of individual privacy.

[23]Pub. L. No. 107-347 (Dec. 17, 2002); Pub. L. No. 113-283 (Dec 18, 2014). See footnote 10 for additional detail.

[24]Office of Management and Budget, *Preparing for and Responding to a Breach of Personally Identifiable Information*, M-17-12 (Washington, D.C.: Jan. 3, 2017).

timelines for notifying affected individuals and reporting to OMB, DHS, and other entities.

DHS addressed these privacy requirements by developing policies and procedures for the protection of PII that is collected, used, or stored by contractors.

DHS Established and Maintains a Comprehensive Privacy Program

DHS has developed a privacy program that includes policies and procedures to ensure that *Privacy Act* requirements apply to contractors, and that contracts and other agreements, such as interagency and international sharing agreements, incorporate privacy requirements.[25] Specifically, DHS's *Privacy Policy and Compliance* directive establishes the privacy policy for the department. The directive includes language requiring contracts and other agreements to incorporate privacy requirements and for department contractors to follow the policy.[26]

Further, the department's *Homeland Security Acquisition Regulation* requires the insertion of a contract clause regarding certain safeguards when the contractor's employees require access to sensitive information.[27] Also, DHS's *Class Deviation 15-01 from the Homeland Security Acquisition Regulation: Safeguarding of Sensitive Information* requires the insertion of two special clauses in contracts and solicitations that have a high risk of unauthorized access to or disclosure of sensitive information, of which PII is a subset.[28] The clauses pertain to the safeguarding of sensitive information and IT security and privacy training. The safeguarding of sensitive information clause is included when a contract is designated as high risk by the program manager, in

[25]5 U.S.C. § 552a.

[26]Department of Homeland Security, *Privacy Policy and Compliance*, 047-01 (Washington, D.C.: July 7, 2011).

[27]Department of Homeland Security, *Department of Homeland Security Acquisition Regulation* (Washington, D.C.: Feb. 2019). 48 C.F,R Subpart 3024.1 states that procedures for implementing the *Privacy Act* are contained in DHS regulations under 6 C.F.R. Part 5, Subpart B.

[28]Department of Homeland Security, *Class Deviation 15-01 from the Homeland Security Acquisition Regulation: Safeguarding of Sensitive Information* (Washington, D.C.: March 2015).

coordination with the component head of contracting activity, the chief information officer, the chief security officer, and the privacy officer. The clause, among other things, addresses safeguarding requirements for privacy information, the contractor's breach notification, and privacy incident response responsibilities.

DHS Requires Agency-wide Privacy Training for All Employees and Contractors

DHS's *Privacy Policy Guidance Memorandum* states that the department is to provide training to all employees and contractors who have access to or use PII.[29] In addition, the department's *Privacy Policy and Compliance* instruction document states that all DHS employees and contractors are required to complete annual online privacy training. Further, the instruction document states that employees, including contractors, who handle sensitive PII are to receive additional, role-based privacy training. Lastly, it states that component privacy officers are responsible for overseeing component privacy training and providing educational materials, consistent with mandatory and supplementary training developed by the Chief Privacy Officer.

DHS Established Processes to Oversee Privacy in Information Systems Operated by Contractors

To oversee information systems, including those operated by contractors, DHS established a privacy compliance process that is outlined in the department's *Privacy Policy Guidance Memorandum* and Privacy Compliance Review Standard Operating Procedure.[30] Specifically, the process consists of four areas: privacy threshold analysis (PTA), privacy impact assessment (PIA), system of records notice (SORN), and periodic review.

For the PTA, the DHS Privacy Office is required to review artifacts to determine if a contractor-operated system is privacy-sensitive and requires additional privacy compliance documentation, such as in a PIA or SORN. If deemed necessary, the privacy office within a component

[29]Department of Homeland Security, *Privacy Policy Guidance Memorandum*, 2017-01 (Washington, D.C.: April 25, 2017).

[30]Department of Homeland Security, *Privacy Compliance Review Standard Operating Procedure* (Washington, D.C.: Nov. 2016).

agency is required to develop a PIA, which, among other things, identifies privacy risks for systems and programs and identifies mitigation strategies for those risks. Similarly, if deemed necessary, DHS is required to develop a SORN, which provides the public notice, among other things, regarding PII collected in a system of records.

Moreover, once the PTA, PIA, and SORN have been completed, the DHS Privacy Office is required to review them periodically. The review entails the assessment of a system's compliance with current privacy documentation and applicable DHS policies. For example, if a program has memorandums of understanding or other information sharing access agreements with contractors or third parties, the DHS Privacy Office is to assess compliance with the terms.

DHS also developed a policy to maintain an inventory of information systems that includes systems used or operated by contractors on behalf of the department. Specifically, DHS developed a systems policy directive which states that the department is required to use its PTA process to maintain a current inventory listing of information systems identified for collecting, using, maintaining, or sharing PII. In addition, the directive states that components are to ensure that the information systems inventory is updated, as needed, and provide the list to DHS annually.

DHS Established Policies to Ensure Implementation of Privacy Controls for Contractor Information Systems

The *DHS 4300A Sensitive Systems Handbook* provides guidance and best practices for the implementation of information systems.[31] Specifically, the handbook includes checklists of required and recommended measures that protect the privacy of the department's information, including information maintained by contractors. The handbook outlines, among other things, the privacy controls that facilitate DHS's efforts to comply with privacy requirements. Also, the handbook notes that contractors share in the responsibility of protecting sensitive information and must adhere to the same standards as the federal government uses.

[31]Department of Homeland Security, *DHS 4300A Sensitive Systems Handbook*, version 12.0 (Washington, D.C.: Nov. 15, 2015).

In addition to the handbook, DHS's *Class Deviation 15-01 from the Homeland Security Acquisition Regulation: Safeguarding of Sensitive Information*[32] identifies two special clauses that are to be included in contracts that have a high risk of unauthorized access to or disclosure of sensitive information, of which PII is a subset. The clause on safeguarding of sensitive information states that the contractor is to follow all current versions of government policies and guidance, including NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*. Further, the clause states that contractors are to have an independent third party validate the security and privacy controls in place for a system. These controls include governance, privacy requirements for contractors, privacy monitoring, training, and information sharing.

DHS Developed Privacy Incident Response Procedures for Contractor Information Systems

DHS developed the *Privacy Incident Handling Guidance*, which supports the department's efforts to safeguard information contained in all department information systems, including ones maintained by contractors. The guidance instructs its components, employees, senior officials, and contractors of their obligation to protect PII.[33] Specifically, when DHS personnel, which includes contractors, discover a suspected or confirmed privacy incident, the guidance outlines a series of actions and activities that must occur to appropriately report, investigate, respond to, and mitigate the privacy incident. The guidance also includes, among other things, timelines for notifying affected individuals and reporting to OMB and other entities. For example, if the privacy incident is determined to be a major incident, the DHS Chief Privacy Officer is required to notify Congress within 7 days and to issue a report with additional information within 30 days. Moreover, the guidance includes a broad range of mitigation strategies based on the nature and sensitivity of the PII involved, which includes, but is not limited to, the notification to affected individuals, the public, and the media.

[32]Department of Homeland Security, *Class Deviation 15-01 from the Homeland Security Acquisition Regulation: Safeguarding of Sensitive Information* (Washington, D.C.: March 9, 2015).

[33]Department of Homeland Security, *Privacy Incident Handling Guidance*, 047-01-008 (Washington, D.C.: Dec. 4, 2017).

Components Followed Oversight Requirements for Privacy Controls in Contractor-Operated Systems, but Some Controls Were Not Fully Implemented

According to NIST, assessing privacy controls is an important element of privacy oversight. In addition, OMB's annual FISMA reporting instructions require agencies to develop policies and procedures for agency officials to follow when overseeing how their contractors implement privacy controls on contractor-operated systems.

NIST also developed related privacy controls and associated activities that agencies should complete. In accordance with federal oversight requirements, DHS developed policies and procedures for overseeing the implementation of privacy controls in systems, including contractor-operated systems, that collect, use, maintain, or share PII.[34] These oversight requirements and associated activities are outlined in table 1.

Table 1: Department of Homeland Security (DHS) Oversight Activities Required for the Implementation of Privacy Controls in Contractor-Operated Systems

Oversight requirements	Related privacy controls	Associated activities
Establish and maintain a comprehensive privacy program	Establish privacy requirements	• Establish roles and responsibilities for protecting personally identifiable information (PII) in policies • Define privacy requirements in contracts to ensure that agencies can hold contractors accountable
	Identify and address gaps in privacy compliance	• Identify and address gaps in privacy compliance by conducting assessments
Provide privacy training for employees, including contractors	Develop and administer privacy training for contractors	• Develop and implement a comprehensive training policy • Administer annual privacy training and targeted role-based privacy training (where necessary) and ensure that contractors understand their responsibilities for privacy requirements
	Maintain PII inventory of contractor information systems	• Establish and maintain an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing PII

[34]Department of Homeland Security, *DHS 4300A Sensitive Systems Handbook*, version 12 (Washington, D.C.: Nov. 15, 2015) and *Class Deviation 15-01 from the Homeland Security Acquisition Regulation: Safeguarding of Sensitive Information* (Washington, D.C.: Mar. 9, 2015).

Oversight requirements	Related privacy controls	Associated activities
Establish oversight procedures to ensure implementation of privacy controls	Outline and evaluate information sharing with contractors and third parties	• Provide information to contractors that describes the PII in their possession and specifically describe the purposes for which the PII may be used • Evaluate any proposed new instances of sharing PII with third parties to assess whether the sharing has been authorized

Source: GAO analysis based on DHS and National Institute of Standards and Technology guidance. | GAO-22-104144

Table 2 shows DHS components' compliance with the activities associated with key controls.

Table 2: Assessment of Selected Department of Homeland Security (DHS) Components' Oversight of the Implementation of Privacy Controls in Selected Contractor-Operated Systems

Associated activities	CBP	DHS HQ	FEMA	ICE	TSA	USCG
Establish roles and responsibilities for protecting personally identifiable information (PII) in policies	Met	Met	Met	Met	Met	Met
Define privacy requirements in contracts to ensure that agencies can hold contractors accountable	Met	Met	Met	Met	Met	Met
Identify and address gaps in privacy compliance by conducting assessments	Met	Met	Met	Met	Met	Not met
Develop and implement a comprehensive training policy	Met	Met	Met	Met	Met	Met
Administer annual privacy training and targeted role-based privacy training (where necessary) and ensure that contractors understand their responsibilities for privacy requirements	Met	Partially met	Met	Met	Met	Partially met
Establish and maintain an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing PII	Met	Met	Met	Met	Met	Met
Provide information to contractors that describes the PII in their possession and specifically describe the purposes for which the PII may be used	Met	Met	Met	Met	Met	Met
Evaluate any proposed new instances of sharing PII with third parties to assess whether the sharing has been authorized	Met	Met	Met	Met	Not met	Not met

CBP = Customs and Border Protection, DHS HQ = Department of Homeland Security headquarters, FEMA = Federal Emergency Management Agency, ICE = Immigration and Customs Enforcement, TSA = Transportation Security Administration, USCG = United States Coast Guard

Met = met associated activities; partially met = partially met associated activities; not met = did not meet associated activities

Source: GAO analysis of agency-provided data. | GAO-22-104144

Overall, with a few exceptions, the selected components we reviewed had generally complied with the requirements for overseeing the

implementation of privacy controls in contractor-operated systems. Specifically, all six components had established privacy requirements by outlining roles and responsibilities for contractor personnel who handle PII and by defining privacy requirements in contracts that we reviewed. In addition, all of the components had developed and implemented a comprehensive training policy for contractors. Further, all components had maintained an inventory of the programs and systems that housed collected, used, or shared PII. Lastly, the six components provided information to contractors that described the PII in their possession and how the PII may be used.

However, DHS HQ did not demonstrate that it provided targeted role-based privacy training to its contractors. In addition, USCG did not demonstrate that it was able to identify and address gaps in privacy compliance; it also did not demonstrate whether contractors understood their responsibilities for privacy requirements. Further, USCG and TSA did not demonstrate that proposed new instances of sharing personally identifiable information with third parties were fully documented.

All Components Established Privacy Requirements for Their Contractors

All of the selected components had established policies outlining privacy roles and responsibilities for contractor personnel who handle PII for the specific contracts we reviewed. For example, FEMA's policies described the roles and responsibilities of employees and contractors and the processes required to ensure that operations comply with privacy best practices, such as developing and conducting PTAs and reporting any suspected or confirmed breach of privacy data.

Further, all of the selected components had defined privacy requirements for protecting PII in the contracts we reviewed. For example, ICE's contract stated that the contractor must comply with DHS's privacy policies regarding the collection, use, retention, and dissemination of PII. In addition, ICE included specific privacy requirements in its contract related to limiting access to sensitive information, privacy training for contractors, safeguarding PII, and remediation of privacy incidents.

Most Components Identified and Addressed Gaps in Contractors' Privacy Compliance

Five out of six of the selected components—CBP, DHS HQ, FEMA, ICE, and TSA—identified and addressed gaps in compliance for the systems we reviewed. Each component conducted PTAs, which determined whether the systems contained PII, described the PII collected by the system, and described how the PII was to be used in order to identify and address gaps in privacy compliance.[35]

The assessments also allowed the components to identify gaps in the PII being collected and the uses of that PII. For example, CBP conducted a PTA for the contractor-operated system we reviewed. The PTA identified that a new application was being used for a purpose different than the one specified in the contract-related documentation. As a result, CBP developed a new PIA to help mitigate any risks to PII.

For the sixth component, the USCG Privacy Officer described the mechanism for reviewing systems. However, USCG did not provide documentation of this process.[36] The same official stated that USCG was drafting an overarching PIA that will be used to identify and assess the agency's use of medical-related government and contractor systems, but did not provide a time frame for completing this documentation. Until USCG ensures privacy compliance assessments are fully documented, the PII contained in contractor systems are at increased risk of unauthorized disclosure.

[35]A privacy threshold analysis identifies an IT system and/or technology that involves PII, describes what PII is collected, and how that information is used. A privacy threshold analysis is required whenever a new information system is being developed or an existing system is significantly modified.

[36]According to DHS guidance, a privacy compliance review is a process designed to provide a constructive mechanism to improve a DHS program's ability to comply with assurances made in existing privacy compliance documentation including privacy impact assessments and system of records notices. Department of Homeland Security, *Privacy Compliance Reviews* (Washington, D.C., Jan. 19, 2017).

All Components Developed and Administered Privacy Training for Contractors, but Two Did Not Complete All Associated Activities

All six components developed and implemented training policies that required contractors to take annual privacy training before accessing agency systems. For example, TSA policy required that all contractors complete annual privacy training that discusses how to handle PII, data protection, and incident response. In addition, contractors at USCG were required to take the annual DHS privacy training prior to gaining access to its systems.

However, while all of the components administered and ensured that basic privacy training was provided to contractors, one component did not provide targeted role-based privacy training and one component did not demonstrate that it ensured that its contractors that worked on the systems we reviewed, understood their responsibilities for privacy requirements. Specifically:

- Five components—CBP, FEMA, ICE, TSA, and USCG—administered targeted role-based privacy training, where necessary, to their contractors working on the systems we reviewed. For example, CBP required its contractors to take role-based training for contractors that had system access privileges above those of a regular user in order to access or use PII. Also, USCG required its contractors that would be accessing or using protected health information in the system we reviewed to take *Health Insurance Portability and Accountability Act* (HIPAA) training.[37]

  On the other hand, DHS headquarters officials stated that the component implements role-based training as needed, but they did not require role-based training for the system we reviewed. However, while DHS indicates role-based training is to be implemented as needed, according to NIST guidance, it is important to provide role-based training to employees, including contractors, accessing PII so they understand their responsibilities to protect the PII based on their assigned roles. Until DHS headquarters provides targeted role-based

[37]HIPAA authorized the Secretary of HHS to promulgate regulations to protect the privacy of certain health information and also required the establishment of security standards. The HIPAA regulations require that covered entities only use or disclose protected health information in a manner permitted by the regulations. 42 U.S.C. §§ 1320d-1320d-8. The HIPAA Privacy and Security Rules were promulgated at 45 C.F.R. Parts 160 and 164.

privacy training to contractors that have responsibility for protecting PII for the system we reviewed, the component lacks full assurance that PII is being adequately protected.

- Five components—CBP, DHS headquarters, FEMA, ICE, and TSA—provided documentation that showed that their contractors working on the systems we reviewed understood their responsibilities regarding privacy requirements. For example, FEMA provided a list of contractors that completed the training for the system we selected, which indicated that they understood the training material.

  USCG stated that the contractors that had received training understood their responsibilities, but it did not provide documentation to support this assertion. Without ensuring contractors certify their acceptance of the responsibilities for meeting privacy requirements, component officials lack assurance that contractors understand their detailed responsibilities for protecting PII.

All Components Maintained a PII Inventory of Contractor-Operated Information Systems

All of the components established and maintained an inventory that contained a listing of all programs and information systems identified for collecting, using, maintaining, or sharing PII. The inventory included the respective systems we reviewed at each component. For example, ICE had documented its inventory using PTAs that listed all IT systems that contain PII. In addition, CBP submits its PTAs to the DHS Privacy Office to help populate an inventory of systems that contain PII.

All Components had a Process for Evaluating New Uses of PII, but Two Components Lacked Such a Process

All components outlined and evaluated information that was shared with contractors and third parties. Specifically, the components described the PII and the approved purposes for which the PII may be used. For example, ICE outlined the type of PII shared with the contractor and the specific uses for this information in its Interface Control Agreement for the system we reviewed. In addition, USCG described the specific PII and the specific purposes for which the PII may be used in its System of Records Notice for the system we reviewed.

Further, four components—CBP, DHS headquarters, FEMA, and ICE—either evaluated or had a process in place to evaluate whether proposed new instances of sharing PII with third parties was authorized. For example, for the system we reviewed, FEMA conducted a PTA to evaluate proposed new sharing of PII with third parties. In addition, ICE evaluated proposed new instances of sharing PII in the system we reviewed by consulting with relevant stakeholders to solicit comments and feedback on the PII. As a result of conferring with the stakeholders, ICE developed a Letter of Intent to approve the sharing of PII with another government agency. Specifically, the letter identified the purpose for sharing, the specific use of the data, and the list of PII to be shared.

Officials from two components—TSA and USCG— stated that there were no proposed new instances of sharing PII with third parties for the systems we reviewed. The TSA privacy official stated that the mechanism for such evaluations would have taken place at change request meetings. For USCG, its privacy official stated that contractual relationships provide for how and with whom PII can be shared. However, neither component provided documentation that specified the process in place to evaluate proposed new instances of sharing PII. Without ensuring the authorization of proposed new instances of sharing PII is documented, the components face an increased risk that contractors will use the shared PII without proper authorization.

Most DHS Components Implemented Procedures to Identify, Remediate, and Share Lessons Learned

NIST and OMB provide guidelines to agencies for responding to privacy incidents. According to NIST, agencies are to establish an effective incident response program that allows for detecting, analyzing, prioritizing, and handling incidents. OMB guidance instructs agencies to ensure that incident response procedures are in place for information systems used or operated by contractors on behalf of the agency.

Accordingly, DHS developed the *Privacy Incident Handling Guidance* (PIHG), which informs its components, employees, senior officials, and contractors of their obligation to protect PII.[38] Specifically, the guidance

[38]Department of Homeland Security, Privacy Office, *Privacy Incident Handling Guidance*, 047-01-008 (Washington, D.C.: Dec 4, 2017).

outlines the department's process for how privacy incidents are to be identified and remediated, and for how lessons learned are to be developed and shared with other components. According to the guidance, a series of key actions and activities must be performed to appropriately identify, remediate, and identify lessons learned for privacy incidents, including those that occur within contractor-operated systems.

Of the six selected components, four components had privacy incidents that resulted in a breach of data during the time frame of July 1, 2018 through June 30, 2019. Three of the four selected components fully identified, remediated, and identified and shared lessons learned for the privacy incidents that we reviewed.[39] The remaining component identified and shared lessons learned for the privacy incident we reviewed, but did not fully remediate the incident in accordance with guidance.

All of the Selected Contractor-Related Privacy Incidents Were Identified in a Timely Manner

The PIHG requires all personnel, including contractors, to report a privacy incident immediately on verification. Specifically, each component is required to:

- report the incident to the component's help desk or to the component privacy officials;
- collect the information about the privacy incident that is necessary to open a security event notification; and
- enter the incident into the DHS incident database and assign a priority level within 24 hours

All four components had completed the required activities to identify their respective privacy incidents according to the guidance and in a timely manner. Specifically, each component reported its incidents to the appropriate component privacy officials and collected the necessary information about the incident to create a security event notification in the incident database. For example, TSA's incident intake report identified the date and time the incident was discovered, along with the type of data involved and the number of individuals affected. Further, each component

[39]Two components were not included in our review of handling of privacy incidents. According to DHS-reported data on privacy incidents for the time frame we reviewed, the U.S. Coast Guard did not have a confirmed privacy incident and the Department of Homeland Security headquarters' privacy incident did not result in an actual breach in PII.

entered the incident in the database and assigned the incident a priority level within 24 hours of confirmation of the privacy incident.

Most of the Selected Privacy Incidents Were Remediated in Accordance With Agency Guidance

The PIHG requires all personnel, including contractors, to report a privacy incident immediately on discovery. Specifically, each component should perform the following activities, as appropriate:

- review the contract, if the incident is caused by a contractor, for inclusion of any privacy incident notification or incident response requirements;
- review the incident and applicable documentation, such as the SORN, PIA, and other existing compliance documents, to determine if the incident meets the definition of a major privacy incident;
- conduct a risk assessment to determine the risk of harm to individuals impacted by the privacy incident;
- determine and document the appropriate mitigation steps in the DHS incident database;
- determine recommendations on notification for affected individuals and document them in the database; and
- request incident closure in the database.

Three components—FEMA, ICE, and TSA—had completed all of the appropriate activities required to remediate their selected incidents in accordance with DHS guidance. The remaining component—CBP—took some steps to remediate the privacy incidents, but did not complete all of them. Specifically:

- All of the components reviewed the respective contract for the inclusion of incident notification or response requirements.[40] For example, CBP privacy officials stated that they reviewed and verified that their contract contained the appropriate clauses, which included,

[40]We deemed this criterion to be not applicable to FEMA's privacy incident because during the investigation of the incident, FEMA determined the contractor was not at fault for the incident. FEMA privacy officials stated that they determined that the component had shared more information than was needed with the contractor, therefore they had no need to review the contract for notification or incident response requirements.

but were not limited to, the incident response clause for sensitive information and the additional PII notification requirement clause.

- All of the components reviewed the incident and other applicable documentation to determine if their incident met the definition. For example, in a letter to Congress, FEMA reported that its review of the PIA, the SORN, and the Interconnection Security Agreement confirmed its determination of the incident to be a major incident. In addition, CBP used the criteria in OMB guidance to determine that the incident met the definition of a major privacy incident. Lastly, ICE and TSA Privacy Office officials reviewed DHS and OMB guidance to determine that their respective incidents did not meet the definition of a major privacy incident and were, instead, minor incidents.

  All components, with the exception of CBP, updated the incident database with the risk assessment findings for their incidents. For example, FEMA completed the DHS Risk Assessment Checklist, which includes information such as the nature and sensitivity of the PII and the likelihood of access and use of the PII, and uploaded it into the database. While CBP provided documentation of a completed DHS Risk Assessment Checklist, the findings were not up to date in the incident database as required. The CBP Privacy Branch Chief stated that elements of the risk assessment were interspersed throughout the database; however, we determined that some of the elements in the database, specifically the nature and sensitivity of PII, were outdated and did not reflect the most recent findings identified by CBP in its risk assessment. OMB requires that the risk assessment, including the factors the agency considered when assessing the risk, be documented in order to properly escalate and tailor breach response activities. Without having up to date risk assessment findings documented in the incident database, DHS and its components may not be able to ensure that the assessment was accurate and that the appropriate mitigation measures were taken.

- All components updated the incident database with the mitigation steps used to address the incident. For example, CBP, TSA, and FEMA each documented both technical steps and oversight measures, such as additional training for staff and updating standard operating procedures used to mitigate the incident.
- All components, with the exception of CBP, documented recommendations for notification of affected individuals in the incident database. For example, ICE documented its recommendation to not notify affected individuals. According to ICE Privacy Office officials, notification to affected individuals was deemed not necessary

because the risk of harm was low due to the incident being immediately reported to the ICE Security Operations Center. CBP Privacy officials also determined they did not need to notify affected individuals because the risk of harm was low. CBP Privacy officials stated that notification to affected individuals can be annotated in multiple places within the database; however, they did not provide evidence from the database to document their efforts. Without clearly documenting notification recommendations for affected individuals, DHS and its components may not be able to ensure that they are taking all the appropriate steps to lessen potential harm that the loss, compromise, or misuse of the PII could have on affected individuals.

- All of the components documented their requests for closure of the respective incidents in the database, giving DHS privacy officials the ability to systemically review and confirm that the incidents were handled in accordance with DHS guidance. For example, as part of its closure request, FEMA attached to the database, the final close out report to Congress with regard to its privacy incident. Further, ICE provided a summary of the privacy incident, which included information about the root cause of the incident, the remediation steps to fix the incident, and plans going forward to prevent the incident from happening again, as part of its request for closure of the incident.

Further, the PIHG includes specific activities that must be conducted in a timely manner for privacy incidents determined to be a major incident. Specifically, the DHS Chief Privacy Officer is to convene the DHS Breach Response Team within 72 hours and notify the appropriate congressional committees within 7 days and again within 30 days after the incident has been discovered. Each of the two components—CBP and FEMA—that experienced a major privacy incident during the time of our review addressed the specific criteria for these types of incidents.

Lessons Learned for All Privacy Incidents Were Shared

The PIHG outlines steps for components to take to conduct a lessons learned exercise, when appropriate. The lessons learned exercise allows DHS to implement specific, preventative actions to protect and safeguard PII. Specifically, the PIHG states that, for major privacy incidents, DHS is to convene the Breach Response Team to conduct a lessons learned exercise and document any findings in a supplemental report to Congress. For minor privacy incidents, the PIHG states the DHS Chief Privacy Officer will rely on the component's privacy officer to convene a small task group to review the incident or assign the task to the component's Privacy Office incident manager, as appropriate. The

lessons learned exercise should review the incident to determine whether the root cause of the incident can be identified and document the results in the incident database.

Further, the PIHG suggests that component privacy officers work through the DHS Privacy Office to communicate with the other component privacy officers about the privacy incident. This process ensures that the DHS Privacy Office is aware of the incident and that the mitigation and remediation processes are consistent for all components.

All of the components demonstrated that the root causes of their incidents were identified and that lessons learned were documented in the database. For example, FEMA's incident was determined to be a major privacy incident that required the agency to convene a Breach Response Team to determine lessons learned. The team determined the root cause and documented its findings in the database and in a supplemental report to Congress. In this case, ICE determined the root cause to be a software glitch and the component documented that, going forward, a software validation process would be performed as part of their lessons learned.

Additionally, the PIHG suggests that component privacy officers determine whether the privacy incident involves PII from multiple DHS components and designate the incident as a multiple component privacy incident in the DHS incident database. None of the privacy incidents we reviewed were designated as involving multiple components; however, it is an essential step in the lessons learned process, according to the PIHG. Sharing this information is vital to ensure other components are aware of the incident and that the mitigation and remediation of the other components is consistent, where applicable.

To ensure general information on incidents, including lessons learned, are shared among components; the DHS Privacy Office conducts monthly incident practitioner meetings and an annual tabletop exercise, which the DHS components attend. At these meetings, lessons learned from major incidents are discussed, among other things, and components are able to ask questions and provide comments on the incidents. For example, at the 2020 annual tabletop exercise, the DHS Privacy Office shared lessons learned from a major incident and had the DHS Office of the Chief Procurement Officer provide an overview of DHS's *Class Deviation 15-01 from the Homeland Security Acquisition Regulation: Safeguarding of Sensitive Information* to increase components' knowledge and understanding of the special clauses included in the deviation.

Conclusions

The risk of improper access or use of PII data that resides on DHS contractor-operated systems calls for DHS to be increasingly vigilant in implementing and enforcing privacy processes and controls to help mitigate the risk of disclosure or modification of privacy information. Importantly, DHS and the components we reviewed have mostly adhered to key activities for the oversight of privacy controls in contractor-operated systems. Nevertheless, opportunities exist to address gaps in training and documentation to further ensure full compliance with privacy requirements. Regarding incident remediation activities, DHS components identified and reported incidents in a timely manner and most selected privacy incidents were remediated in accordance with agency guidance. However, CBP did not fully document risk assessment findings and recommendations for notifying affected individuals of privacy incidents in the incident database. Until DHS follows through on ensuring that components fully implement key privacy and remediation activities, PII is at increased risk of misuse and insufficient protection.

Recommendations for Executive Action

We are making a total of seven recommendations to DHS and its components, including one to DHS HQ, three to USCG, two to CBP, and one to TSA. Specifically:

The Secretary of the Department of Homeland Security should direct its Privacy Office to provide targeted role-based privacy training to contractors who are responsible for protecting PII. (Recommendation 1)

The Commandant of the U.S. Coast Guard should direct the USCG Privacy Office to establish a time frame to complete the development of a process that can be used to identify and assess the gaps in contractor compliance with privacy requirements. (Recommendation 2)

The Commandant of the U.S. Coast Guard should direct the USCG Privacy Office to ensure, in conjunction with the acquisition office, that contractors certify their acceptance of their privacy requirement responsibilities. (Recommendation 3)

The Commandant of the U.S. Coast Guard should direct the USCG Privacy Office to ensure the evaluation of proposed new instances of

sharing personally identifiable information with third parties are fully documented. (Recommendation 4)

The Commissioner of U.S. Customs and Border Protection should direct the CBP Privacy Office to ensure that risk assessments are fully documented in the incident database. (Recommendation 5)

The Commissioner of U.S. Customs and Border Protection should direct the CBP Privacy Office to ensure that recommendations to notify affected individuals of privacy incidents are fully documented in the incident database. (Recommendation 6)

The Administrator of the Transportation Security Administration should direct the TSA Privacy Office to ensure the evaluation of proposed new instances of sharing personally identifiable information with third parties are fully documented. (Recommendation 7)

Agency Comments and Our Evaluation

DHS provided written comments on a draft of this report. In its comments, which are reproduced in appendix II, the department concurred with our recommendations and described steps planned or under way to address them.

For example, with regard to recommendation 1, the DHS Privacy Office stated that it planned to review its privacy training to determine whether to make specific role-based training for contractors, as appropriate. In addition, with regard to recommendation 3, DHS noted that the USCG Privacy Office planned to collaborate with the acquisition office to ensure that all contractors complete privacy awareness, and other required privacy-related training, as required under contractual clauses.

Further, concerning recommendation 5, the department noted that the CBP Privacy Office planned to collaborate with the DHS Privacy Office on proposed language to update the PIHG. The planned updates include clearly delineating roles for posting finalized risk assessments when an incident is categorized as major and ensuring the requirement to fully document the provision of notice to affected individuals is included in the incident database.

The department also described actions it said it had taken in response to three of our recommendations and requested that we consider these

recommendations to be implemented. Specifically, with regard to our recommendation that the USCG Privacy Office establish a time frame to complete the development of a process that can be used to identify and assess the gaps in contractor compliance with privacy requirements (recommendation 2), the department stated that all new or updated uses of PII are required to be evaluated by a PTA. It added that this analysis is used to determine whether a PIA and/or a SORN is required for the new uses of PII. If required, DHS said the PIAs are the tool used by the Coast Guard to identify and assess gaps in contractor compliance with privacy requirements. For this reason, the department requested that we consider this recommendation to be resolved and implemented.

With regard to our recommendation that the Coast Guard Privacy Office ensure the evaluation of proposed new instances of sharing personally identifiable information with third parties is fully documented (recommendation 4), the department stated that the Coast Guard Privacy Office reviews all contract modifications involving PII pursuant to the Department's Homeland Security Acquisition Manual. Thus, the department requested that we also consider this recommendation resolved and implemented.

Finally, the department requested that we consider resolved and implemented, our recommendation that the TSA Privacy Office ensure the evaluation of proposed new instances of sharing personally identifiable information with third parties is fully documented (recommendation 7). The department stated that the TSA Privacy Office would raise proposed new instances of sharing PII with third parties during monthly meetings between the Contracting Officer Representative and the contractor lead. The department also stated that significant changes would be documented in the DHS PTA.

However, the department did not provide documentation related to any of the described actions that would support the closure of these three recommendations. We intend to follow up with the department to verify the actions it has taken to address the recommendations. DHS also provided technical comments on the draft report, which we incorporated, as appropriate.

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

If you or your staff have any questions about this report, please contact Nick Marinos at (202) 512-9342 or by email at marinosn@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix III.

Sincerely yours,

Nick Marinos
Director, Information Technology and Cybersecurity

Appendix I: Objectives, Scope, and Methodology

The objectives of our review were to determine the extent to which

(1) the Department of Homeland (DHS) has developed policies and procedures for the protection of personally identifiable information (PII) that is collected, used, or stored by contractors;

(2) selected major DHS components oversee the implementation of privacy controls within contractor-operated systems that collect, use, or store PII on behalf of the department; and

(3) DHS components have ensured that privacy incidents occurring in contractor-operated systems are identified and remediated in an effective and timely manner; and that lessons learned are shared with all components, as appropriate.

To address the first objective, we analyzed DHS policies, procedures, and other documentation that describe the department's requirements to protect PII that is collected, used, or stored by contractors. We then compared them to selected privacy requirements specified in relevant federal laws and Office of Management and Budget (OMB) and National Institute of Standards and Technology (NIST) guidance. To identify the requirements, we reviewed federal laws and guidance, such as the *Privacy Act of 1974*,[1] the *E-Government Act of 2002*,[2] the *Federal Information Security Modernization Act of 2014,*[3] the *Federal Acquisition*

[1]*Privacy Act of 1974*, 5 U.S.C. § 552a.

[2]*E-Government Act of 2002*, Pub. L. 107-347 (Dec. 17, 2002).

[3]*Federal Information Security Modernization Act of 2014,* Public Law 113-283 (Dec. 18, 2014).

Regulation,[4] the Office of Management and Budget (OMB) Circular A-130: *Managing Information as a Strategic Resource*,[5] the OMB memorandum on *Preparing for and Responding to a Breach of Personally Identifiable Information* (M-17-12),[6] the National Institute of Standards and Technology (NIST) Special Publication 800-53 Rev. 4: *Security and Privacy Controls for Federal Information Systems and Organizations*[7] and Special Publication 800-37 Rev. 2: *Risk Management Framework for Information Systems and Organizations*.[8] In selecting the practices for our assessment, we focused on those practices identified by federal laws and OMB and NIST guidance that addressed the oversight of contractors that collect, use, or store information on behalf of a government entity. Those practices included establishing a comprehensive privacy program, conducting privacy training, overseeing privacy in information systems operated by contractors, implementing privacy controls, and ensuring that privacy incident response procedures are in place for contractor information systems. We supplemented our analyses with interviews with relevant agency officials, such as the DHS Privacy Office, to gain insight into how DHS's policies and procedures addressed the practices that aim to protect PII that is accessible by contractors.

[4]The FAR establishes uniform policies and procedures for acquisition of supplies and services by executive agencies. The FAR and agency supplements are codified in title 48 of the *Code of Federal Regulations*. As relevant here, the FAR's requirements for acquisitions of information technology are at 48 C.F.R. Part 39. The acquisition planning requirements for IT security are at 48 C.F.R. § 7.103(w). See also, FAR § 7.105(b)(16)(*Government-furnished information*) and (18)(*Security considerations*). FAR Subpart 24.1 address protection of individual privacy. The Homeland Security Acquisition Regulation, at 48 C.F.R. Subpart 3024.1, states that procedures for implementing the *Privacy Act* are contained in DHS regulations under 6 C.F.R. Part 5, Subpart B.

[5]Office of Management and Budget, *Managing Information as a Strategic Resource*, Circular A-130 (July 28, 2016).

[6]Office of Management and Budget, *Preparing for and Responding to a Breach of Personally Identifiable Information*, M-17-12 (Washington, D.C.: Jan. 3, 2017).

[7]National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53 Rev. 4 (Gaithersburg, MD: April 2013). NIST 800-53 Revision 4 has been replaced with Revision 5, but the September 23, 2021, implementation deadline had not occurred when we completed our analysis. Revision 4 was relevant during our reporting period and used as criteria.

[8]National Institute of Standards and Technology, *Risk Management Framework for Information Systems and Organizations*, Special Publication 800-37 Rev. 2 (Gaithersburg, MD: Dec. 2018).

For objectives two and three, we reviewed six major DHS component's efforts to oversee privacy-related issues within contractor-operated systems that collect, use, or store PII on behalf of the department. To select the major DHS components to be included in our review, we requested a list of privacy incidents[9] that occurred in DHS major components' contractor-operated systems from July 1, 2018 through June 30, 2019.[10] From the data DHS provided, we determined that six major components had experienced a privacy incident: U.S. Coast Guard; U.S. Customs and Border Protection; U.S. Department of Homeland Security Headquarters; Federal Emergency Management Agency; U.S. Immigration and Customs Enforcement; and Transportation Security Administration.

To address the second objective, we reviewed relevant documentation pertaining to specific contractor-operated systems at each of the six components we selected for review and compared the information to DHS requirements related to the oversight of privacy controls within those systems. Relevant documentation included, but was not limited to, contracts, privacy impact assessments, privacy threshold analyses, and component privacy policies and procedures. To identify the contractor-operated systems included in our review, we selected from each of the six components, the system that had experienced the highest reported risk level privacy incident during the requested timeframe. In instances where the component had privacy incidents involving PII that had the same risk level, we selected both contractor-operated systems. In order to identify the selected DHS requirements included in our review, we considered those requirements in DHS's *4300A Sensitive Systems Handbook*[11] and

[9]DHS defines a "privacy incident" as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than the authorized user accesses or potentially accesses [PII] or (2) an authorized user accesses or potentially accesses [PII] for an unauthorized purpose. The term encompasses both suspected and confirmed incidents involving PII, whether intentional or inadvertent, which raises a reasonable risk of harm.

[10]The major operational components that currently make up the Department of Homeland Security are: U.S. Citizenship and Immigration Services, U.S. Coast Guard, U.S. Customs and Border Protection, Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security Headquarters, Federal Emergency Management Agency, Federal Law Enforcement Training Center, U.S. Immigration and Customs Enforcement, U.S. Secret Service, and Transportation Security Administration.

[11]Department of Homeland Security, *DHS 4300A Sensitive Systems Handbook*, version 12.0 (Washington, D.C.: Nov. 15, 2015).

acquisition policies that are focused on areas related to the oversight of contractor implementation of privacy controls.

We supplemented our analyses with interviews of relevant agency officials, such as the DHS Privacy Officer, component-level security and privacy officials, and relevant contractor staff, to discuss the oversight of privacy controls in the selected contractor-operated systems. We then determined whether the evidence provided by the agency addressed each identified criteria element. Specifically, for each criteria element, we determined if the evidence fully addressed the element ("met"), addressed some, but not all, aspects of the element ("partially met"), or did not address any aspects of the element ("not met"). We also discussed the results of our initial analysis of documentation with agency officials to validate our findings, collect additional evidence, and identify causes for any gaps.

To address the third objective, we selected four of the six major components to include in our review because they had privacy incidents that resulted in an actual data breach. Of those four major components, we reviewed documentation on specific contractor-related privacy incidents that occurred at the components and compared their documentation to selected DHS requirements related to privacy incident handling and response. Relevant documentation included, but was not limited to, contracts, incident intake reports, incident database reports, systems of record notices, PIAs, risk assessments, lessons learned exercises, and congressional notification letters. To identify the privacy incidents included in our review, we selected the incident with the highest reported risk level within each component during our timeframe. In those instances where there were multiple incidents reported at the highest risk level within a component, we selected the most recent incident. To identify DHS privacy incident handling requirements, we reviewed requirements specified in DHS's *Privacy Incident Handling Guidance* (PIHG) and focused on requirements related to identifying and remediating privacy incidents and sharing lessons learned with other components.[12]

We supplemented our analyses with interviews with relevant agency officials, such as component privacy and information security and contractor staff, to gain additional insight into the steps they took to

[12]Department of Homeland Security, Privacy Office, *Privacy Incident Handling Guidance*, 047-01-008 (Washington, DC: Dec. 4, 2017).

identify and remediate the specific incidents. Additionally, we inquired about the steps they took to share lessons learned with other components. We then determined whether the evidence provided by the agency addressed each identified criteria element. We also discussed the results of our initial analysis of documentation with agency officials to validate our findings, collect additional evidence, and identify causes for any gaps.

We conducted this performance audit from March 2020 to December 2021 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.

Appendix II: Comments from the Department of Homeland Security

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

Homeland Security

November 19, 2021

Nick Marinos
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Management Response to Draft Report GAO-22-104144, "DHS PRIVACY: Selected Component Agencies Generally Provided Oversight of Contractors, but Further Actions Needed to Address Gaps"

Dear Mr. Marinos:

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

The Department is pleased to note GAO's recognition that DHS developed policies and procedures to mitigate the risks to personally identifiable information (PII) on contractor-operated systems, such as: (1) establishing and maintaining a comprehensive privacy program; (2) providing agency-wide privacy training for all employees and contractors; (3) overseeing information systems operated by contractors; (4) ensuring implementation of privacy controls for contractor-operated systems; and (5) ensuring privacy incident response procedures for contractor-operated information systems. DHS remains committed to protecting PII that is collected and maintained, as well as continuing policies and controls to prevent improper PII access and use.

The draft report contained seven recommendations with which DHS concurred. Attached find our detailed response to each recommendation. DHS previously submitted technical comments addressing several accuracy, contextual, and other issues under a separate cover for GAO's consideration.

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

Sincerely,

JIM H CRUMPACKER

Digitally signed by JIM H CRUMPACKER
Date: 2021.11.19 12:26:44 -05'00'

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

Attachment

2

Attachment: Management Response to Recommendations Contained in GAO-22-104144

GAO recommended that the Secretary of the Department of Homeland Security direct the Privacy Office:

Recommendation 1: Provide targeted role-based training to contractors that have responsibility for protecting PII.

Response: Concur. The DHS Privacy Office requires annual agency-wide training for its employees and its contractors, which addresses the proper handling and safeguarding of PII. The training, titled "DHS MANDATORY -Privacy at DHS: Protecting Personal Information," was developed by the DHS Privacy Office in accordance with the Chief Privacy Officer's responsibilities to develop and oversee mandatory and supplementary training outlined in DHS Directive 047-01, "Privacy Policy and Compliance," dated July 7, 2011. The DHS Privacy Office considers this training sufficient with regard to content, but will review the training to determine whether to make specific role-based training for contractors, as appropriate. Estimated Completion Date (ECD): November 30, 2022.

GAO recommended that the Commandant of the U.S. Coast Guard direct the Coast Guard Privacy Office:

Recommendation 2: Establish a time frame to complete the development of a process that can be used to identify and assess the gaps in contractor compliance with privacy requirements.

Response: Concur. In accordance with DHS Directive 047-01, and as applicable to the given contract, all new or updated uses of systems and PII require an initial Privacy Threshold Analysis (PTA). The PTA determines if a Privacy Impact Assessment (PIA) and/or System of Records Notice (SORN) is required, including the creation of a new PIA and/or SORN or updating of existing documentation. PIAs are the tool used by the Coast Guard to identify and assess gaps in contractor compliance with privacy requirements, and are completed, as appropriate.

DHS requests that GAO consider this recommendation resolved and closed, as implemented.

Recommendation 3: Ensure, in conjunction with the acquisition office, contractors certify their acceptance of their privacy requirement responsibilities.

Response: Concur. The Coast Guard Privacy Office will collaborate with the Acquisition Directorate (CG-9) to ensure that all contractors complete privacy awareness, and other required privacy-related training, as required under contractual clauses. Processes will be documented so that Contracting Officers and Contracting Officer Representatives understand the requirements to document the required training. ECD: November 30, 2022.

Recommendation 4: Ensure the evaluation of proposed new instances of sharing personally identifiable information with third parties are fully documented.

Response: Concur. If a contracted services provider proposes to share PII with a third party outside the scope of the contract, the contract would be modified to reflect this new requirement. The Coast Guard Privacy Office reviews all contract modifications involving PII pursuant to the Department's Homeland Security Acquisition Manual, Appendix G, dated October 2009. In the specific contractual relationship for laboratory services assessed by the GAO in this draft report, Coast Guard notes that there were no new proposed uses of PII sharing, given the scope of the contract.

DHS requests that GAO consider this recommendation resolved and closed, as implemented.

GAO recommended that the Commissioner of U.S. Customs and Border Protection (CBP) direct the CBP Privacy Office:

Recommendation 5: Ensure that risk assessments are fully documented in the incident database.

Response: Concur. The CBP Privacy Office will continue to indicate the risk assessment value in the criticality section of the incident record, i.e., Low, Moderate, Significant, Informational, etc., as well as provide relevant information within the incident narrative to inform the risk determination reflected within the content of the incident journal log, as appropriate. The CBP Privacy Office will review all supporting documentation in the incident database, and note in the incident journal whether any final documentation (such as the final risk assessment) needs to be completed, and will coordinate with the DHS Privacy Office to ensure the documents and findings are uploaded by the DHS Privacy Office into the incident database, as appropriate.

The CBP Privacy Office will also collaborate with the DHS Privacy Office on proposed language to update to the DHS Privacy Office's "Privacy Incident Handling Guidance" (PIHG), dated December 4, 2017, related to the handling of incidents involving third party and contractor-involved breaches. This proposed language will include clearly delineated roles for the posting finalized risk assessments and an incident journal input when an incident is categorized as MAJOR/SIGNIFICANT. ECD: November 30, 2022.

4

Recommendation 6: Ensure that recommendations to notify affected individuals of privacy incidents are fully documented in the incident database.

Response: Concur. The CBP Privacy Office, as part of its standing processes, regularly indicates whether notification of affected individuals is part of the incident remediation within the incident journal notes, as well as in the "Remediations Tasks Completed" section of the incident database record. CBP Privacy will continue to work, in conjunction with the DHS Privacy Office, to ensure this information is properly contained in the incident record as part of the review prior to the DHS Privacy Office granting closure of the incidents. In addition, the CBP Privacy Office will collaborate with the DHS Privacy Office to update the PIHG to ensure that the requirement to fully document the provision of notice to affected individuals is included in the incident database. ECD: November 30, 2022.

GAO recommended that the Administrator of the Transportation Security Administration (TSA) direct the TSA Privacy Office:

Recommendation 7: Ensure the evaluation of proposed new instances of sharing personally identifiable information with third parties are fully documented.

Response: Concur. Proposed new instances of sharing PII with third-parties would be raised during monthly meetings between the Contracting Officer Representative and the contractor lead, as required in the Statement of Work for the contract, and significant changes would be documented in the DHS PTA. No new instances of sharing with third-parties were identified for the specific contract covering the data breaches that were reported in 2019, so TSA did not have documentation to provide that a new instance was evaluated. TSA's Privacy Office shared its process with GAO for evaluating new proposed instances of sharing PII with a third party on February 26, 2021, but had no specific instances to specifically document that the process was followed. However, it is important to note that all requirements for an existing process and an established method of documenting such cases when they arise are already in place, which TSA believes meets the intent of this recommendation.

DHS requests that GAO consider this recommendation resolved and closed, as implemented.

5

Text of Appendix II: Comments from the Department of Homeland Security

November 19, 2021

Nick Marinos

Director, Information Technology and Cybersecurity

U.S. Government Accountability Office

441 G Street, NW

Washington, DC 20548

Re: Management Response to Draft Report GAO-22-104144, “DHS PRIVACY: Selected Component Agencies Generally Provided Oversight of Contractors, but Further Actions Needed to Address Gaps”

Dear Mr. Marinos:

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

The Department is pleased to note GAO’s recognition that DHS developed policies and procedures to mitigate the risks to personally identifiable information (PII) on contractor- operated systems, such as: (1) establishing and maintaining a comprehensive privacy program; (2) providing agency-wide privacy training for all employees and contractors; (3) overseeing information systems operated by contractors; (4) ensuring implementation of privacy controls for contractor-operated systems; and (5) ensuring privacy incident response procedures for contractor-operated information systems. DHS remains committed to protecting PII that is collected and maintained, as well as continuing policies and controls to prevent improper PII access and use.

The draft report contained seven recommendations with which DHS concurred. Attached find our detailed response to each recommendation. DHS previously submitted technical comments addressing several accuracy, contextual, and other issues under a separate cover for GAO’s consideration.

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

Sincerely,

JIM H. CRUMPACKER, CIA, CFE

Director

Departmental GAO-OIG Liaison Office

Attachment

Attachment: Management Response to Recommendations Contained in GAO-22-104144

GAO recommended that the Secretary of the Department of Homeland Security direct the Privacy Office:

Recommendation 1: Provide targeted role-based training to contractors that have responsibility for protecting PII.

Response: Concur. The DHS Privacy Office requires annual agency-wide training for its employees and its contractors, which addresses the proper handling and safeguarding of PII. The training, titled "DHS MANDATORY - Privacy at DHS: Protecting Personal Information," was developed by the DHS Privacy Office in accordance with the Chief Privacy Officer's responsibilities to develop and oversee mandatory and supplementary training outlined in DHS Directive 047-01, "Privacy Policy and Compliance," dated

July 7, 2011. The DHS Privacy Office considers this training sufficient with regard to content, but will review the training to determine whether to make specific role-based training for contractors, as appropriate. Estimated Completion Date (ECD): November 30, 2022.

GAO recommended that the Commandant of the U.S. Coast Guard direct the Coast Guard Privacy Office:

Recommendation 2: Establish a time frame to complete the development of a process that can be used to identify and assess the gaps in contractor compliance with privacy requirements.

Response: Concur. In accordance with DHS Directive 047-01, and as applicable to the given contract, all new or updated uses of systems and PII require an initial Privacy Threshold Analysis (PTA). The PTA determines if a Privacy Impact Assessment (PIA) and/or System of Records Notice (SORN) is required, including the creation of a new PIA and/or SORN or updating of existing documentation. PIAs are the tool used by the Coast Guard to identify and assess gaps in contractor compliance with privacy requirements, and are completed, as appropriate.

DHS requests that GAO consider this recommendation resolved and closed, as implemented.

Recommendation 3: Ensure, in conjunction with the acquisition office, contractors certify their acceptance of their privacy requirement responsibilities.

Response: Concur. The Coast Guard Privacy Office will collaborate with the Acquisition Directorate (CG-9) to ensure that all contractors complete privacy awareness, and other required privacy-related training, as required under contractual clauses.

Processes will be documented so that Contracting Officers and Contracting Officer Representatives understand the requirements to document the required training. ECD: November 30, 2022.

Recommendation 4: Ensure the evaluation of proposed new instances of sharing personally identifiable information with third parties are fully documented.

Response: Concur. If a contracted services provider proposes to share PII with a third party outside the scope of the contract, the contract would be modified to reflect this new requirement. The Coast Guard Privacy Office reviews all contract modifications involving PII pursuant to the Department's Homeland Security Acquisition Manual, Appendix G, dated October 2009. In the specific contractual relationship for laboratory services assessed by the GAO in this draft report, Coast Guard notes that there were no new proposed uses of PII sharing, given the scope of the contract.

DHS requests that GAO consider this recommendation resolved and closed, as implemented.

GAO recommended that the Commissioner of U.S. Customs and Border Protection (CBP) direct the CBP Privacy Office:

Recommendation 5: Ensure that risk assessments are fully documented in the incident database.

Response: Concur. The CBP Privacy Office will continue to indicate the risk assessment value in the criticality section of the incident record, i.e., Low, Moderate, Significant, Informational, etc., as well as provide relevant information within the incident narrative to inform the risk determination reflected within the content of the incident journal log, as appropriate. The CBP Privacy Office will review all supporting documentation in the incident database, and note in the incident journal whether any final documentation (such as the final risk assessment) needs to be completed, and will coordinate with the DHS Privacy Office to ensure the documents and findings are uploaded by the DHS Privacy Office into the incident database, as appropriate.

The CBP Privacy Office will also collaborate with the DHS Privacy Office on proposed language to update to the DHS Privacy Office's "Privacy Incident Handling Guidance" (PIHG), dated December 4, 2017, related to the handling of incidents involving third party and contractor-involved breaches. This proposed language will include clearly delineated roles for the posting finalized risk assessments and an incident journal input when an incident is categorized as MAJOR/SIGNIFICANT. ECD: November 30, 2022.

Recommendation 6: Ensure that recommendations to notify affected individuals of privacy incidents are fully documented in the incident database.

Response: Concur. The CBP Privacy Office, as part of its standing processes, regularly indicates whether notification of affected individuals is part of the incident remediation within the incident journal notes, as well as in the "Remediations Tasks Completed" section of the incident database record. CBP Privacy will continue to work, in conjunction with the DHS Privacy Office, to ensure this information is properly contained in the incident record as part of the review prior to the DHS Privacy Office granting closure of the incidents. In addition, the CBP Privacy Office will collaborate with the DHS Privacy Office to update the PIHG to ensure that the requirement to fully document the provision of notice to affected individuals is included in the incident database. ECD: November 30, 2022.

GAO recommended that the Administrator of the Transportation Security Administration (TSA) direct the TSA Privacy Office:

Recommendation 7: Ensure the evaluation of proposed new instances of sharing personally identifiable information with third parties are fully documented.

Response: Concur. Proposed new instances of sharing PII with third-parties would be raised during monthly meetings between the Contracting Officer Representative and the contractor lead, as required in the Statement of Work for the contract, and significant changes would be documented in the DHS PTA. No new instances of sharing with third- parties were identified for the specific contract covering the data breaches that were reported in 2019, so TSA did not have documentation to provide that a new instance was evaluated. TSA's Privacy Office shared its process with GAO for evaluating new proposed instances of sharing PII with a third party on February 26, 2021, but had no specific instances to specifically document that the process was followed. However, it is important to note that all requirements for an existing process and an established method of documenting such cases when they arise are already in place, which TSA believes meets the intent of this recommendation.

DHS requests that GAO consider this recommendation resolved and closed, as implemented.

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Nick Marinos, (202) 512-9342 or marinosn@gao.gov

Staff Acknowledgments

In addition to the contact named above, Marisol Cruz Cain (Assistant Director), Elena Epps (Analyst-in-Charge), Amy Apostol, Kami Brown, Chris Businsky, Breanne Cave, Nancy Glover, Monica Perez-Nelson, Priscilla Smith, and Marshall Williams, Jr. made key contributions to this report.

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/about/what-gao-does/fraudnet

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

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@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

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