OFFICE OF INSPECTOR GENERAL

DHS Privacy Office Needs to Improve Oversight of Department-wide Activities, Programs, and Initiatives

Homeland Security

November 4, 2020
OIG-21-06

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

November 4, 2020

MEMORANDUM FOR: Dena Kozanas
Chief Privacy Officer
Department of Homeland Security

FROM: Joseph V. Cuffari, Ph.D.
Inspector General

JOSEPH V CUFFARI
Digitally signed by JOSEPH V CUFFARI
Date: 2020.11.04 14:56:24 -05'00'

SUBJECT: *DHS Privacy Office Needs to Improve Oversight of Department-wide Activities, Programs, and Initiatives*

Attached for your action is our final report, *DHS Privacy Office Needs to Improve Oversight of Department-wide Activities, Programs, and Initiatives*. We incorporated the formal comments provided by your office.

The report contains three recommendations aimed at improving the DHS Privacy Office. Your office concurred with all three recommendations. Based on information provided in your response to the draft report, we consider recommendations 1 through 3 open and resolved. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions. Please send your response or closure request to OIGAuditsFollowup@oig.dhs.gov.

Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

Please call me with any questions, or your staff may contact Sondra McCauley, Assistant Inspector General for Audits, at (202) 981-6000.

DHS OIG Highlights

DHS Privacy Office Needs to Improve Oversight of Department-wide Activities, Programs, and Initiatives

November 4, 2020

Why We Did This Audit

Congress enacted the *Privacy Act of 1974* (Privacy Act) and *E-Government Act of 2002*. These Acts specifically require agencies collecting, using, or disseminating personally identifiable information to prevent unwarranted invasions of privacy. OIG is legislatively mandated to periodically assess the agency's implementation of the Privacy Act. Our audit objective was to determine whether the DHS Privacy Office has effective oversight of department-wide privacy activities, programs, and initiatives.

What We Recommend

We made three recommendations to the DHS Privacy Office to improve oversight of privacy compliance, information sharing access agreements, and privacy training.

For Further Information:
Contact our Office of Public Affairs at (202) 981-6000, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov

What We Found

Although the Department of Homeland Security Privacy Office established a comprehensive framework to administer its privacy program, it does not yet have effective oversight of department-wide privacy activities, programs, and initiatives. The DHS Privacy Office has established policies, procedures, and guidance for components to carry out mission duties in accordance with Privacy Act requirements. However, the DHS Privacy Office has not conducted adequate oversight to ensure consistent execution of its privacy program across DHS components.

Specifically, the DHS Privacy Office has not established controls to ensure that privacy compliance documentation and Information Sharing Access Agreements are completed and submitted as required. The DHS Privacy Office also did not monitor completion of required privacy training across the Department. These shortfalls existed because the DHS Privacy Office did not have sufficient measures in place to ensure DHS components adhered to its privacy program. Without such measures, DHS may not be able to identify and address new privacy risks in existing systems and programs or prevent inappropriate dissemination of personally identifiable information.

DHS Privacy Office Response

DHS concurred with all three recommendations. Appendix B contains DHS' management comments in their entirety.

Table of Contents

Appendixes

Abbreviations

CBP	U.S. Customs and Border Protection
CPO	Chief Privacy Officer
FEMA	Federal Emergency Management Agency
ICE	U.S. Immigration and Customs Enforcement
IQ	Internet Quorum
ISAA	Information Sharing Access Agreement
IT	information technology
OMB	Office of Management and Budget
PII	personally identifiable information
PIA	Privacy Impact Assessment
PPOC	Privacy Points of Contact
PRIV-CATS	Privacy Compliance Artifact Tracking System
PTA	Privacy Threshold Analysis
SORN	System of Records Notice
TSA	Transportation Security Administration
U.S.C.	United States Code
USCIS	U.S. Citizenship and Immigration Services

Background

The Federal Government collects personally identifiable information (PII) from members of the public and may share that information with other agencies and partners to carry out missions mandated by Federal statute. The Office of Management and Budget (OMB) defines PII as information (e.g., name, address, phone number) that can be used to distinguish or trace an individual's identity, either alone or combined with information that is linked or linkable to a specific individual. Social security numbers and financial account numbers are considered even more sensitive because if lost, compromised, or disclosed without authorization, the breach could result in substantial harm or unfairness to an individual.

Congress enacted the *Privacy Act of 1974*[1] (Privacy Act) and the *E-Government Act of 2002*[2] (E-Government Act) to balance the Government's access and collection of PII with the protection of individuals from unwarranted invasions of privacy. The Acts impose specific requirements on agencies when collecting PII. The E-Government Act requires agencies to address privacy risks when developing or procuring new or modified technologies to collect, maintain, use, or disseminate PII. Additionally, agencies must fully protect individual privacy and comply with the Privacy Act and all other applicable privacy laws, regulations, and policies when sharing data.

In its mission to secure the homeland, the Department of Homeland Security collects PII from U.S. citizens, lawful permanent residents, and foreign nationals visiting the United States. DHS employees and contractors may share that information with its partners, including other Federal agencies and state and local governments, to carry out day-to-day mission duties. For example, the Federal Emergency Management Agency (FEMA) collects PII from disaster survivors and may share limited PII with its partners with disaster mission responsibility. U.S. Customs and Border Protection (CBP) collects PII from foreign nationals when processing passengers at ports of entry to target high-risk travelers and facilitate legitimate travelers. All DHS information technology (IT) systems, programs, and initiatives that collect PII or have privacy impact are subject to the requirements of U.S. data privacy and disclosure laws.

[1] *Privacy Act of 1974*, 5 United States Code (U.S.C.) 552a, as amended.
[2] *E-Government Act of 2002*, 44 U.S.C. 101.

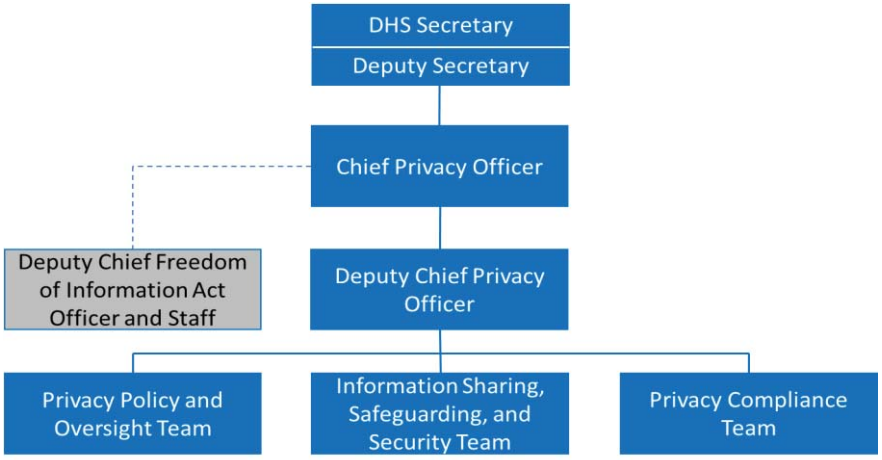
DHS Privacy Organization

The DHS Chief Privacy Officer (CPO) heads the DHS Privacy Office and serves as the Department's Senior Agency Official for Privacy. The CPO has primary responsibility for privacy policy at DHS, which includes ensuring the use of technology does not erode privacy protections. Specifically, the CPO's responsibilities include:

- establishing, overseeing the implementation of, and issuing guidance on DHS privacy policy;
- ensuring the Department follows DHS privacy policy and Federal government-wide privacy laws and policies;
- reviewing and approving all Department privacy compliance documentation to ensure that privacy considerations are addressed when planning or updating any IT systems and programs used at DHS;
- ensuring that all DHS information-sharing agreements comply with DHS privacy compliance documentation requirements and DHS privacy policy;
- investigating and mitigating privacy incidents; and
- developing and overseeing privacy training throughout DHS.

The DHS Privacy Office's mission is to protect individuals by embedding and enforcing privacy protections and transparency in all DHS activities. The Privacy Office organization chart[3] is shown in Figure 1.

Figure 1. DHS Privacy Office Organization Chart



Source: Office of Inspector General (OIG) created to highlight privacy-specific teams

[3] The DHS Privacy Office includes a Deputy Chief Freedom of Information Act Officer and teams responsible for *Freedom of Information Act* policy and compliance. These functions were not included in this audit and, therefore, are not described in this report.

The DHS Privacy Office includes three teams, under a Deputy CPO, responsible for establishing and implementing privacy policy:

1) The Privacy Policy and Oversight Team is responsible for developing DHS privacy policy. The team conducts internal privacy compliance reviews and privacy investigations, manages privacy incident response, and oversees the handling of privacy complaints. The team also supports the privacy training, public outreach, and reporting functions of the DHS Privacy Office.

2) The Information Sharing, Safeguarding, and Security Team provides specialized privacy expertise to support DHS information-sharing initiatives with its partners. The team also evaluates information sharing requests to assess and mitigate privacy risks and ensure compliance with privacy terms and conditions.

3) The Privacy Compliance Team oversees privacy compliance activities, including supporting DHS component privacy officials and programs. Compliance activities include the review and approval of privacy compliance documentation to ensure that privacy considerations are addressed when planning or updating any IT systems and programs used at DHS.

Component heads are responsible for implementing DHS privacy policies and procedures and assisting the DHS CPO with addressing privacy incidents and complaints within DHS offices and components (collectively referred to as components). DHS privacy policy requires certain components to each appoint a Component Privacy Officer.[4] The Component Privacy Officer reports directly to the component head and oversees the privacy compliance policy and oversight activities. Component Privacy Points of Contact (PPOC) assume the duties of Component Privacy Officers in components that do not have privacy officers. The Component Privacy Officer's responsibilities include:

- serving as the DHS CPO's main point of contact;

[4] DHS Instruction 047-01-005, *Component Privacy Officer*, February 6, 2017, requires the following components each appoint a privacy officer: CBP, FEMA, Office of Intelligence and Analysis, U.S. Immigration and Customs Enforcement, National Protection Programs Directorate, Science and Technology Directorate, Transportation Security Administration, United States Coast Guard, U.S. Citizenship and Immigration Services, Federal Law Enforcement Training Centers, Office of Operations Coordination, and United States Secret Service.

- maintaining ongoing review of all component IT systems and programs, information sharing, and other activities to identify collections and uses of PII and any other attendant privacy impacts;
- coordinating with system and program managers and the CPO to complete required privacy compliance documentation;
- overseeing component implementation of DHS and component privacy policy, including procedures and guidance for handling suspected and confirmed privacy incidents; and
- overseeing component privacy training.

OIG and the U.S. Government Accountability Office have previously conducted audits of privacy stewardship within DHS components and identified compliance issues related to privacy protection laws, regulations, policies, information sharing, and training. See Appendix C for examples of the resulting privacy audit reports. We conducted this audit to determine whether the DHS Privacy Office demonstrated effective oversight of department-wide privacy activities, programs, and initiatives.

Results of Audit

Although the DHS Privacy Office established a comprehensive framework to administer its privacy program, it does not yet have effective oversight of department-wide privacy activities, programs, and initiatives. The DHS Privacy Office has established policies, procedures, and guidance for components to carry out mission duties in accordance with the Privacy Act requirements. However, the DHS Privacy Office has not conducted adequate oversight to ensure consistent execution of its privacy program across DHS components.

Specifically, the DHS Privacy Office has not established controls to ensure that privacy compliance documentation and Information Sharing Access Agreements (ISAA) are completed and submitted as required. The DHS Privacy Office also did not monitor the completion of required privacy training across the Department. These shortfalls existed because the DHS Privacy Office did not have sufficient measures in place to ensure DHS components adhered to its privacy program. Without such measures, DHS may not be able to identify and address new privacy risks in existing systems and programs or prevent inappropriate dissemination of PII.

The DHS Privacy Office Established a Framework for Administering a Department-wide Privacy Program

The DHS Privacy Office established a comprehensive framework to protect PII handled through department-wide activities, programs, and initiatives, as required by Federal law and OMB. Specifically, the DHS Privacy Office developed policies and guidance for (1) assessing the privacy impacts of IT systems and programs that involve PII, (2) responding to privacy incidents, and (3) providing ongoing privacy awareness training to DHS employees and contractors.

Assessing Privacy Impacts

The E-Government Act requires agencies to conduct Privacy Impact Assessments (PIA) before developing or procuring IT systems or projects that collect, maintain, or disseminate PII.[5] A PIA is an analysis of the handling of PII to ensure alignment with applicable privacy requirements, determine the privacy risks associated with an information system or activity, and evaluate ways to mitigate privacy risks.

Accordingly, the DHS Privacy Office has developed and implemented privacy policies, procedures, and guidance to assess the privacy impacts of IT systems and programs. Specifically, the DHS Privacy Office implemented a privacy compliance process that includes the review and approval of three key documents: Privacy Threshold Analysis (PTA), PIA, and System of Records Notice (SORN). The DHS Privacy Office has also developed detailed guidance and templates to standardize the preparation of PTAs, PIAs, and SORNs, which are available on the DHS Privacy Office's internal website. The following describes the three key privacy compliance documents:

> Privacy Threshold Analysis – A PTA must be prepared before implementing or modifying all IT systems and programs that may involve PII or otherwise impact the privacy of individuals. A PTA includes a general description of the system or program and describes what PII is collected, from whom, and how that information is used. The Department uses the PTA to identify programs and systems that are privacy-sensitive and determine whether additional privacy compliance documentation, such as a PIA or SORN, is required.
>
> Privacy Impact Assessment – A PIA is used to identify and mitigate privacy risks at the beginning and throughout the development life cycle

[5] *E-Government Act of 2002*, Section 208.

of a system or program, and is required before a system or program containing PII becomes operational. The PIA also provides an analysis of the privacy considerations posed and the steps taken to mitigate any impact on privacy. A PIA describes:

- what information is collected and why;
- how the information will be used, stored, shared, and accessed;
- how the information will be protected from unauthorized use or disclosure; and
- how long the information will be retained.

System of Records Notice – A SORN is the official public notice of a system of records as required by the Privacy Act. A system of records is a group of records under the control of any Federal agency from which information is retrieved by a unique personal identifier assigned to an individual. SORNs explain how the information is used, retained, and may be corrected, and whether certain portions of the system are subject to Privacy Act exemptions for law enforcement, national security, or other reasons.

The DHS privacy compliance process begins when component program and system managers, in coordination with the Component Privacy Officer, prepare PTAs and submit them to the DHS Privacy Office for review. Privacy Office personnel enter data from PTAs into their Internet Quorum (IQ) project management system to track privacy compliance documentation. Specifically, personnel record the component name, the name of the system or program, the date the PTA was received from the component, and the date the DHS Privacy Office approved the PTA.

If the DHS Privacy Office determines during its PTA review that a PIA is required, the relevant component managers and Privacy Officer draft a PIA and submit it to the DHS Privacy Office for review and approval by the CPO. Privacy Office personnel update the information in IQ by recording the PIA with the corresponding PTA. The Department publishes approved PIAs on its external website,[6] unless they are classified.

During both the PTA and PIA review process, the DHS Privacy Office, in coordination with the Component Privacy Officer, will determine whether a new SORN is required or an existing SORN covers the program or system. Similar to the handling of PTAs and PIAs, the component drafts the SORN, provides it

[6] https://www.dhs.gov/publications-library/collections/privacy-impact-assessments-%28pia%29.

to the DHS Privacy Office for review and approval, and records it in IQ. The Department publishes approved SORNs on the Department's external website[7] and in the Federal Register.

Responding to Privacy Incidents

OMB requires that agencies develop and implement a breach response plan that includes the agency's policies and procedures for reporting, investigating, and managing a breach of PII. OMB defines a breach, which is a type of privacy incident, as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence when (1) a person other than an authorized user accesses or potentially accesses PII, or (2) an authorized user accesses or potentially accesses PII for an unauthorized purpose.[8]

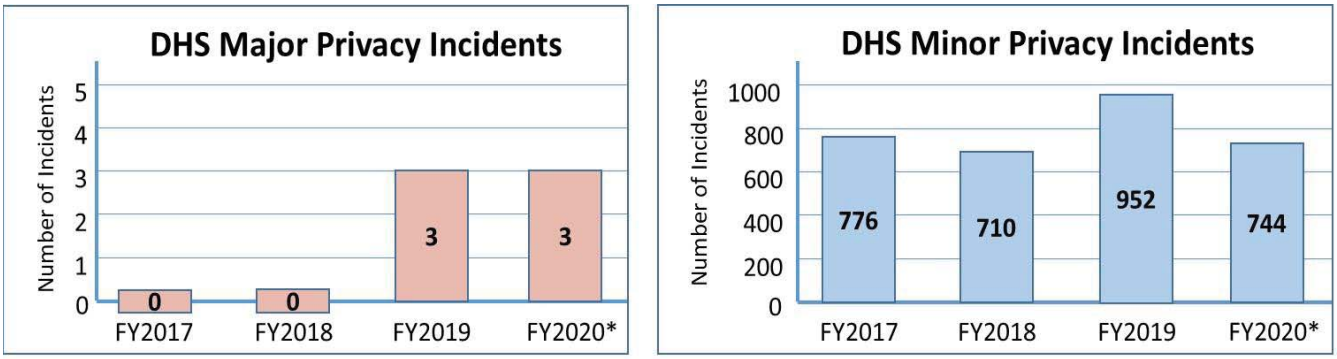
DHS defines a privacy incident as either a major or a minor incident. An incident is deemed "major" when it involves PII of more than 100,000 individuals that, if exfiltrated,[9] modified, deleted, or otherwise compromised, is likely to result in harm to the national security interests, foreign relations, or economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people. A minor incident adversely affects the confidentiality, integrity, or availability of a noncritical system or non-sensitive data, or relates to a minor policy violation. The DHS Privacy Office reported 6 major and 3,182 minor privacy incidents within the Department for fiscal years 2017 through May 27, 2020, as shown in Figure 2.

[7] https://www.dhs.gov/publications-library/collections/system-of-records-notices-%28sorns%29.

[8] OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, January 3, 2017. OMB defines an "incident" as an occurrence that actually or imminently jeopardizes the integrity, confidentiality, or availability of information or an information system, or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. The Department's definition for "privacy incident" comports with OMB's definition of a "breach"; therefore, DHS uses the term "privacy incident" synonymously with the term "breach" for its policies and instructions.

[9] Exfiltration is the unauthorized copying, transfer, or retrieval of data from a computer or server.

Figure 2. DHS Privacy Incidents – FYs 2017–2020



Source: OIG created from data reported by the DHS Privacy Office
*Totals for FY 2020 are as of May 27, 2020.

DHS has implemented a privacy incident program to report, investigate, mitigate, and remediate privacy incidents. Specifically, the DHS Privacy Office has established policies and defined the roles and responsibilities of the specific headquarters and component officials responsible for responding to all incidents involving PII.[10] In addition, the DHS *Privacy Incident Handling Guidance* describes specific procedures for reporting, investigating, and managing a breach of PII.[11]

When DHS personnel discover a suspected or confirmed PII incident, the CPO, in coordination with other DHS officials, determines whether the incident is a minor or major incident involving PII. If minor, the Component Privacy Officer, in coordination with the DHS CPO, handles the investigation, notification, and mitigation. If major, the CPO, who serves as the senior DHS official responsible for oversight of privacy incident management, must notify the Congress and may convene a Breach Response Team. The team includes officials such as the DHS Undersecretary for Management, Chief Information Officer, Chief Information Security Officer, General Counsel, and other DHS officials and component representatives.

In all incidents, the Breach Response Team or Component Privacy Officer assesses the risk of harm to individuals impacted by the privacy incident and the likelihood that the PII is accessible and usable. They also identify appropriate mitigations and make recommendations to the DHS CPO regarding required notifications to affected individuals, which the CPO provides to the DHS Secretary for consideration.

[10] DHS Directive 047-01, *Privacy Policy and Compliance*, July 7, 2011; DHS Instruction 047-01-006, *Privacy Incident Responsibilities and Breach Response Team*, December 4, 2017.
[11] DHS Instruction Guide 047-01-008, *Privacy Incident Handling Guidance*, December 4, 2017.

During this audit, we observed the DHS Privacy Office's handling of one CBP and three FEMA privacy incidents. In accordance with its policy, the DHS Privacy Office designated the incidents as "major" and convened and coordinated a Breach Response Team to manage each incident. The team, led by the CPO, held weekly meetings with the impacted stakeholders to respond to the incidents, and the Department submitted the required congressional notifications timely.

Providing Privacy Awareness Training

OMB requires that agencies develop, maintain, and implement mandatory agency-wide privacy awareness and training programs for all employees and contractors. Further, agencies shall ensure that privacy training is consistent with applicable policies, standards, and guidelines.[12]

The DHS Privacy Office has implemented a privacy-training program throughout the Department. Specifically, the Privacy Office develops and delivers a variety of ongoing and one-time privacy training to DHS personnel and key stakeholders, including new employee training, privacy briefings, and role-based training.

Additionally, the DHS Privacy Office has developed a mandatory annual online privacy awareness training entitled "Privacy at DHS: Protecting Personal Information." DHS provides this annual training to DHS employees through performance and learning management systems. The training is available on the Department's external website so that contractors can access and complete the course before they begin work at DHS. We reviewed the content of the annual online training and determined that it appropriately defines PII; provides information on what is involved in collecting, using, sharing, and safeguarding PII; provides examples of the potential consequences of not protecting PII; and instructs personnel on how to report suspected or confirmed privacy incidents.

The DHS Privacy Office Did Not Ensure Consistent Execution of Privacy Policies and Procedures Department-wide

The DHS Privacy Office has not conducted adequate oversight to ensure consistent execution of its policies and procedures across DHS components. Specifically, the DHS Privacy Office has not (1) performed periodic reviews of all existing IT systems and programs for new or evolving privacy risks, (2) obtained and reviewed all ISAAs involving PII, and (3) ensured that all employees and

[12] OMB Circular No. A-130, *Managing Information as a Strategic Resource*, July 28, 2016.

contractors throughout DHS completed annual privacy awareness training. These shortfalls exist because the Privacy Office did not have sufficient measures in place to ensure DHS components are adhering to privacy policies and guidance. Ineffective oversight of the Department's information-sharing activities may lead to inappropriate dissemination of PII.

DHS Privacy Office Did Not Perform Periodic Reviews for New or Evolving Privacy Risks

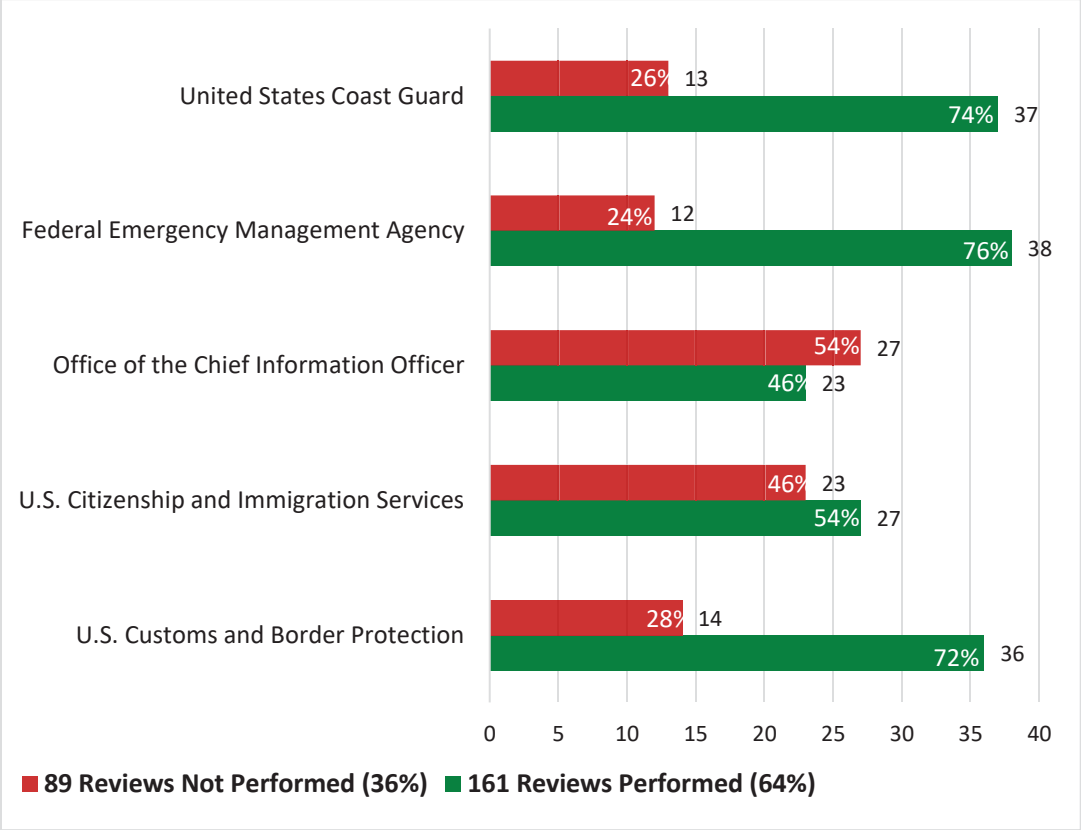
The E-Government Act requires agencies to update PIAs as necessary when a system change creates new privacy risks.[13] As a measure of compliance, DHS privacy policy requires the CPO to schedule a review of existing PTAs and PIAs at least every 3 years, and to notify the relevant Component Privacy Officer or PPOC of the review.[14]

When a PTA is approved, the DHS Privacy Office enters an expiration date into IQ to indicate when the periodic review is due. For PTAs that do not require a PIA, the Office establishes an expiration date 3 years from the PTA approval date. If the DHS Privacy Office determines that a PIA is required and one does not exist, or an existing PIA requires an update, the Office establishes an expiration date 1 year from the PTA approval date to allow sufficient time to draft a PIA. The DHS Privacy Office does not establish expiration dates for PIAs. Instead, the DHS Privacy Office reviews PIAs concurrently with review of the related PTAs.

The DHS Privacy Office did not perform periodic reviews of compliance documentation for all of its existing programs and systems according to policy. The DHS Privacy Office provided an IQ report containing 5,361 PTAs and 360 PIAs approved from January 1, 2014, through September 25, 2019. Five components had a combined total of 3,548 PTAs, accounting for 66 percent of the total PTAs. The review date had passed for about 37 percent, or 1,301 of the PTAs, which were no longer valid. We selected 250 of the expired PTAs for further evaluation, including 50 from each of the 5 components.[15] The DHS Privacy Office had not performed reviews for 89 of 250 (36 percent) of the PTAs. Figure 3 shows the number and percent of the PTAs reviewed by the components in our sample.

[13] *E-Government Act of 2002*, Section 208.
[14] DHS Instruction 047-01-001, *Privacy Policy and Compliance*, July 25, 2011.
[15] Our sampling methodology is described in detail in Appendix A: Objective, Scope, and Methodology.

Figure 3. Number and Percent of Selected PTAs Reviewed Within Five DHS Components



Source: OIG analysis based on information received from DHS component officials
*Displayed percentages are rounded.

Additionally, 85 of the total 360 PIAs, approved from January 1, 2014, through September 25, 2019, were reviewed and approved more than 3 years ago, despite the requirement to review PIAs at least every 3 years. DHS Privacy Office officials did not review 4 of the 85 PIAs because they were associated with expired PTAs. The four PIAs are as follows:

- DHS Wide PIA-045 - Loaned Executive Program
- DHS Operations PIA-004(f) - Publicly Available Social Media Monitoring and Situational Awareness Initiative
- DHS Science and Technology PIA-029 - Centralized Hostile Intent
- DHS TSA PIA-011 - Airmen Certificate Vetting Program.

We further evaluated the remaining 81 PIAs to determine the reasons for the deficiencies, but were unable to reach conclusions based on the data provided by the DHS Privacy Office.

The DHS Privacy Office did not perform timely reviews, in part, because its IQ system did not have automated controls for scheduling recurring reviews of existing PTAs and PIAs. Specifically, the IQ system did not have the capability to alert DHS Privacy Office personnel of expiring PTAs in order to trigger new reviews. Consequently, the DHS Privacy Office did not notify the Component Privacy Officers about pending PTA and PIA reviews. Instead, DHS Privacy Office personnel relied on Component Privacy Officers to notify the DHS Privacy Office about changes to existing PTA and PIA documentation that would require new reviews.

According to a DHS Privacy Office official, the office has not had a distinct process in place to facilitate consistent and recurring PIA reviews since 2014. Since that time, the increasing amount of privacy compliance documentation has made it too burdensome to hold separate PIA reviews. Instead, the DHS Privacy Office has relied on the PTA review process to satisfy the PIA review requirement. The DHS Privacy Office did not record the dates when periodic reviews for PIAs were completed in IQ. Therefore, Privacy Office personnel could not readily determine, from the information in IQ, whether the reviews had been performed.

On October 1, 2019, the DHS Privacy Office implemented a new project management system. The Privacy Compliance Artifact Tracking System (PRIV-CATS) improves the tracking of expiring PTAs by enabling privacy analysts to generate reports of PTAs expiring within 90 days. However, PRIV-CATS does not contain the dates of completed PIA reviews. At the time of our audit in March 2020, the Privacy Office was recording historical PTAs from IQ in PRIV-CATS. However, all pre-existing PIAs and SORNs were uploaded in PRIV-CATS before the system launched in October 2019. According to Privacy Office personnel, it will take some time before all of the data is available in PRIV-CATS to help the office catch up on all delinquent reviews. Without scheduling and performing the required periodic reviews, the DHS Privacy Office cannot proactively identify and mitigate new and evolving privacy risks in existing systems and programs department-wide.

DHS Did Not Review All Information Sharing Access Agreements Containing PII

OMB requires that agencies comply with the Privacy Act and all other applicable privacy laws, regulations, and policies when sharing data.[16] DHS formally documents information sharing activities in an ISAA. ISAAs are defined as any memorandum of understanding, memorandum of agreement, or

[16] OMB Memorandum M-11-02, *Sharing Data While Protecting Privacy*, November 3, 2010.

any form of agreement used to facilitate the exchange of information between two or more parties. ISAAs contain specific requirements relating to privacy, including:

- the appropriate authorities providing the information to the recipient and the recipient collecting the information;
- compliance with provider and recipient privacy documentation requirements; and
- acknowledgment that collection, use, maintenance, and dissemination of PII under the agreement is consistent with each agency's written privacy and civil liberties protection policies.

According to a 2011 DHS privacy policy,[17] the CPO is responsible for ensuring all DHS ISAAs comply with DHS privacy compliance documentation requirements and DHS policy. Additionally, the accompanying instruction[18] calls for Component Privacy Officers and PPOCs, and other DHS employees as appropriate, to submit all proposed ISAAs involving PII to the DHS CPO for review and approval prior to finalizing them. The DHS Privacy Office has developed a specialized PTA template components should use to conduct privacy compliance assessments of ISAAs. This template is available on the DHS Privacy Office's internal website.

Nevertheless, the DHS Privacy Office did not check to ensure it obtained and reviewed all ISAAs involving PII throughout the Department. According to Privacy Office officials, the DHS Privacy Office only reviews ISAAs as they are submitted by the components, without taking additional steps to identify ISAAs that are not submitted. A DHS privacy official explained that, because there is no mechanism to alert the office about ISAAs, they rely solely on the components to submit them as required. As a result, we were unable to determine how many ISAAs exist throughout DHS, and could not validate the extent to which DHS components were in compliance with the 2011 privacy policy.

We conducted an independent review to determine the extent to which each component submitted ISAAs involving PII to the DHS Privacy Office for review. We requested a list of ISAAs from the five selected component privacy offices as well as information on individual ISAA review processes. Four of the five components did not provide any of their ISAAs to the Privacy Office for review. The remaining component provided only some of its ISAAs to the Privacy Office.

[17] DHS Directive 047-01, *Privacy Policy and Compliance*, July 7, 2011.
[18] DHS Instruction 047-01-001, *Privacy Policy and Compliance*, July 25, 2011.

Although two components were unable to provide the audit team the lists, the total ISAAs for the remaining three components, which provided us with the list, totaled more than 2,000.

The DHS Privacy Office had not effectively communicated to all components the requirement to submit ISAAs involving PII to the Privacy Office for review and approval. Consequently, not all Component Privacy Officers were aware of this requirement or the process for submitting the ISAAs. Lacking awareness, one component privacy official told us that components were not required to notify the DHS Privacy Office upon entering into sharing agreements. Therefore, this component did not involve the DHS Privacy Office in its ISAA process. Another component privacy official stated that the requirement to submit ISAAs prior to execution was informally communicated during a meeting with the DHS Privacy Office and, therefore, was not heeded. In addition, a different component official stated that the DHS Privacy Office formally communicated the importance of submitting ISAAs involving PII to the DHS Privacy Office during a privacy compliance review at that component. However, the formal report from the privacy compliance review did not mention instructions or procedures for submitting ISAAs.

Furthermore, one Component Privacy Officer who did not provide ISAAs to the DHS Privacy Office started an independent internal review of all component ISAAs during the course of this audit. The Component Privacy Officer attributed the need for this internal review to findings contained in a March 2019 OIG report on management of PII.[19] The ongoing internal review of this component's ISAAs has already resulted in the discovery of four major privacy incidents.

Without reviewing and approving all ISAAs as required, the DHS Privacy Office cannot ensure DHS is sharing and protecting PII appropriately. Ineffective oversight of the Department's information sharing activities may lead to inappropriate dissemination of PII.

DHS Did Not Ensure Completion of Annual Privacy Training

According to DHS privacy policy,[20] all DHS employees and contractors must complete annual online privacy training. DHS privacy directives and instructions require the CPO to develop and oversee department-wide mandatory and supplementary privacy training. Further, Component Privacy

[19] *Management Alert – FEMA Did Not Safeguard Disaster Survivors' Sensitive Personally Identifiable Information (REDACTED),* OIG-19-32, March 15, 2019.
[20] DHS Instruction 047-01-001, *Privacy Policy and Compliance*, July 25, 2011, and DHS Instruction 047-01-005, *Component Privacy Officer*, February 6, 2017.

Officers or PPOCs are required to conduct and keep records of completed privacy training for employees and contractors in coordination with the DHS Privacy Office. Each year, the Department "assigns" all staff the mandatory annual privacy training in its learning management system. Staff have 1 year to complete the training after it is assigned.

The DHS Privacy Office has not effectively monitored the completion of annual privacy training. As such, when we inquired, the DHS Privacy Office was not aware of the number of employees and contractors who did not complete the training within the required timeframe. According to a DHS Privacy Office official, the DHS Privacy Office collects information on Department training activities to fulfill periodic congressional reporting requirements. Prior to each reporting period, the DHS Privacy Office requests that the Office of the Chief Human Capital Officer and each component provide information on the types of training completed and the total number of attendees. However, the DHS Privacy Office does not request or obtain exception reports for the employees or contractors who do not complete the annual privacy training.

Information we compiled from headquarters and major component training officials indicated that not all DHS employees and contractors completed the annual privacy awareness training within the required timeframe for the past several years. Specifically, more than 50 percent of headquarters staff did not complete the training in 2019. In total, more than 32,000 headquarters and component staff did not complete the training in 2019. See Table 1 for the number and percent of staff at headquarters and major components who did not complete annual privacy awareness training within the required timeframe from 2017 through 2019.

Table 1. Number and Percent of Staff Not Completing Annual Privacy Awareness Training from 2017 through 2019

Office/ Component	2017		2018		2019	
	Number	Percent*	Number	Percent*	Number	Percent*
Headquarters	4,850	57%	4,466	49%	4,845	51%
CBP	9,216	16%	9,313	15%	4,033	6%
FEMA	12,747	72%	14,265	71%	7,292	36%
U.S. Immigration and Customs Enforcement (ICE)	1,908	8%	3,535	13%	3,993	16%
Transportation Security Administration (TSA)	3,743	8%	5,290	10%	2,283	4%
United States Coast Guard	8,373	15%	6,581	12%	7,301	13%
U.S. Citizenship and Immigration Services (USCIS)	3,648	14%	3,304	12%	1,677	6%
United States Secret Service	No data		969	14%	773	12%
Total	**44,485**	**19%**	**47,723**	**18%**	**32,197**	**12%**

Source: OIG analysis of information from DHS training officials
*Percent of staff not completing the training compared with the total number of staff assigned training. Percentages are rounded. See Appendix D for additional information.

The number of staff who did not complete the training within the required timeframe decreased by 6 percent from 2018 to 2019. Specifically, four components (CBP, FEMA, TSA, and USCIS) each reduced the number and percentage of staff not completing training by about 50 percent. It is important to note that these numbers may include staff who took the training subsequent to the report or who left DHS employment before completing the training. However, the number of staff without training warrants attention and monitoring by the DHS Privacy Office.

The DHS Privacy Office has not developed a process to oversee Component Privacy Officers' and PPOCs' monitoring of mandatory annual privacy training. Therefore, the office was unaware of the number of DHS staff who did not complete the training within the required timeframe. The DHS Privacy Office relied solely on the components to ensure their employees and contractors completed the training. We noted the DHS Privacy Office evaluated training compliance during its internal privacy compliance reviews of some components. However, the DHS Privacy Office did not have an ongoing process in place to monitor the completion of all annual privacy training.

Routine training is a key element of developing and maintaining an effective privacy culture. DHS employees and contractors must understand how to

safeguard PII. Without effective oversight to ensure employees and contractors are adequately informed about privacy requirements, the Department's PII is susceptible to breaches. For example, OIG recently reported that FEMA experienced a privacy breach in FY 2019 by releasing to a contractor the PII and sensitive PII of 2.3 million survivors of hurricanes Harvey, Irma, and Maria and the California Wildfires.[21] In response to our report, FEMA officials stated they would modify the contract to include training on management of PII and Sensitive PII. OIG conducted additional audit work to determine whether personnel involved in this incident completed the mandatory privacy training.

Recommendations

We recommend the DHS Chief Privacy Officer:

Recommendation 1: Develop and implement an automated process to initiate and schedule timely and periodic reviews of Privacy Threshold Analyses and Privacy Impact Assessments consistent with the DHS Privacy Office policy.

Recommendation 2: Develop, implement, and formally communicate a process to ensure review of all proposed Information Sharing Access Agreements involving personally identifiable information.

Recommendation 3: Develop and implement a process to monitor the completion of mandatory annual privacy training.

Management Comments and OIG Analysis

DHS concurred with all three of our recommendations. Appendix B contains a copy DHS' response in its entirety. DHS also provided technical comments and suggested revisions to our report in a separate document. We reviewed the technical comments and made changes to the report where appropriate. A summary of DHS' response and our analysis follows.

DHS Comments to Recommendation 1: Concur. Prior to the initiation of this OIG audit, the DHS Privacy Office identified the need for a new compliance tracking system with automated reporting features to track and schedule timely reviews of privacy compliance documents (i.e., PTAs, PIAs, and SORNs).

[21] *FEMA Did Not Safeguard Disaster Survivors Sensitive Personal Identifiable Information,* OIG-19-32, March 2019.

Accordingly, the DHS Privacy Office began working with the DHS Office of the Chief Information Officer on a new tracking system, PRIV-CATS, which the Privacy Office launched in October 2019.

The DHS Privacy Office's prior tracking system, Internet Quorum, did not have a way to capture privacy compliance document renewal requirements or expirations accurately. Further, the system reporting metrics were difficult to extract and decipher. The new system, PRIV-CATS, allows the Privacy Office to extract privacy compliance documents that are expired or set to expire in 30, 60, or 90-day increments and provide appropriate awareness to DHS Component Privacy Offices.

In August 2020, through an extensive manual process, the DHS Privacy Office completed uploading PTAs from 2017 into PRIV-CATS. The Privacy Office is continuing to upload its pre-2017 PTAs. All historical DHS PIAs and SORNs were uploaded into the system prior to its launch in October 2019. The DHS Privacy Office's estimated timeline for implementing this recommendation is to (1) upload historical PTAs from 2014–2017 into PRIV-CATS by September 30, 2021, and (2) upload historical PTAs from 2010–2013 into PRIV-CATS by March 31, 2022. Overall Estimated Completion Date (ECD): March 31, 2022.

OIG Analysis of DHS Comments: The steps DHS has taken satisfy the intent of this recommendation. We consider this recommendation open and resolved until DHS provides documentation to support its completion of planned corrective actions.

DHS Comments to Recommendation 2: Concur. In 2011, when DHS originally published DHS Directive 047-01, *Privacy Policy and Compliance*, and DHS Instruction 047-01-001, *Privacy Policy and Compliance,* the DHS Privacy Office was beginning to understand and build its role in the Department's information sharing process. The Privacy Office now has a greater knowledge of the size and scope of the Department's ISAAs. Because the Department has developed and entered into a high volume of ISAAs, it is not feasible for the DHS Privacy Office to review each agreement. Therefore, the DHS Privacy Office will develop standards for which types of ISAAs the CPO needs to review, and which may be delegated to Component Privacy Officers or PPOCs. The DHS Privacy Office's overall timeline for completion is August 31, 2021.

OIG Analysis of DHS Comments: The steps DHS has taken satisfy the intent of this recommendation. We consider this recommendation open and resolved until DHS provides documentation to support completion of planned corrective actions.

DHS Comments to Recommendation 3: Concur. DHS Instruction 047-01-001 requires that, "All DHS employees and contractors complete annual online privacy training developed by the Chief Privacy Officer or by Component Privacy Officers or PPOCs in consultation with the Chief Privacy Officer." However, the DHS Privacy Office does not have access to individual Component Learning Management Systems to track mandatory annual privacy training across the DHS enterprise. Further, several DHS components have differing required completion dates for their annual privacy training, which makes Headquarters tracking and reporting more difficult.

Regardless of these challenges, the DHS Privacy Office agreed that a better process to monitor the completion of mandatory annual privacy training is necessary. Therefore, the DHS Privacy Office will work with the DHS Office of the Chief Human Capital Officer to develop a technical solution that ensures the DHS Privacy Office receives the statistics it needs on mandatory annual privacy training. The DHS Privacy Office will also consult with the DHS Privacy Council, composed of DHS Component Privacy Officers and PPOCs, to identify potential interim solutions while the technical solution is developed with the Office of Chief Human Capital Officer. ECD: April 30, 2021.

OIG Analysis of DHS Comments: The steps DHS has taken satisfy the intent of this recommendation. We consider this recommendation open and resolved until DHS provides documentation to support completion of planned corrective actions.

Appendix A
Objective, Scope, and Methodology

Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Public Law 107−296), which amended the *Inspector General Act of 1978*. Our audit objective was to determine whether the DHS Privacy Office has effective oversight of department-wide privacy activities, programs, and initiatives.

To accomplish our objective, we obtained and reviewed relevant Federal privacy laws, OMB requirements, as well as U.S. Government Accountability Office and OIG audit reports. We also obtained and reviewed DHS privacy policies, procedures, and guidance. We interviewed Privacy Office officials to gain an understanding of their responsibilities, compliance, and oversight processes. We also contacted Component Privacy Officers and PPOCs from the following components to gain an understanding of their implementation of DHS privacy policies:

U.S. Customs and Border Protection	Office of the Chief Human Capital Officer
Office of the Chief Information Officer	Transportation Security Administration
Federal Emergency Management Agency	United States Coast Guard
U.S. Immigration and Customs Enforcement	U.S. Citizenship and Immigration Services
Office of Biometric Management	United States Secret Service
Office of Intelligence and Analysis	

To determine whether the Department established privacy policies according to Federal laws and OMB requirements, we reviewed the requirements contained in OMB Circular No. A-130, *Managing Information as a Strategic Resource*, Appendix II. During our audit, we assessed the Department's compliance with DHS policies, information provided by the DHS Privacy Office, and information on DHS internal and external websites.

We obtained an IQ report from the DHS Privacy Office of PTAs and PIAs approved from January 1, 2014, through September 25, 2019, to determine whether the DHS Privacy Office performed periodic reviews of PTAs and PIAs. The list contained 5,361 PTAs. We sorted the list by component and determined that 5 components had 3,548 PTAs, which accounted for 66 percent of the total PTAs. We identified 1,580 of the 3,548 PTAs as expired. In some instances, there were multiple PTAs for a single system. We considered the oldest PTAs for each system as "duplicate" entries and removed them from the universe, thereby reducing the universe to 1,301 expired PTAs. Using a

random number generator, we selected a judgmental sample of 250 PTAs, including 50 from each of 5 major components. The number of total and expired PTAs for the five components is shown in Table 2.

Table 2. Number of PTAs in Five Selected Components

Component	Total PTAs	Total Expired PTAs	Less: Duplicate Expired PTAs	Total Unique Expired PTAs	Sampled PTAs
USCIS	1,046	550	120	430	50
CBP	895	325	64	261	50
FEMA	655	352	54	298	50
Coast Guard	541	185	19	166	50
Office of Chief Information Officer	411	168	22	146	50
Total	3,548	1,580	279	1,301	250

Source: OIG-prepared based on data provided by the DHS Privacy Office

The IQ report contained a total of 360 PIAs, including 85 PIAs that were initially reviewed and approved more than 3 years prior to September 25, 2019, and should have had periodic reviews. We selected all 85 PIAs for evaluation.

We judgmentally selected and obtained information from five components — CBP, FEMA, USCIS, Coast Guard, and Secret Service — to determine the extent to which the components provided ISAAs to the DHS Privacy Office for review and approval. We did not review classified or intelligence community information sharing during this audit. Only three of the five components — Secret Service, USCIS, and FEMA — provided us the lists of their ISAAs. FEMA officials stated the list was incomplete or not comprehensive. Only one of the five components provided information on its processes for reviewing ISAAs.

To determine whether all Department employees and contractors completed mandatory annual privacy training within the required timeframe, we obtained information from the Office of the Chief Human Capital Officer for staff from headquarters and seven components — CBP, FEMA, ICE, TSA, Coast Guard, USCIS, and Secret Service. We judgmentally selected these seven components based on privacy and privacy training concerns identified in prior OIG reports. Specifically, we obtained the number of employees and contractors who were assigned training, completed the training, and did not complete the training within the required timeframe for 2017, 2018, and 2019. We have included the data provided in Appendix D.

We obtained a listing of PTAs and PIAs from the DHS Privacy Office and data about privacy training completion from DHS Headquarters and component training officials. We did not perform data reliability testing on this data or perform tests to assess the completeness or accuracy of the data. Rather, we presented the information only as background and context. The scope of this audit was limited to assessing the effectiveness of the DHS Privacy Office's oversight of privacy activities and programs. We assessed controls related to the DHS Privacy Office's processes for reviewing PTAs and PIAs; obtaining, reviewing, and approving ISAAs; and monitoring privacy training. We identified control weaknesses, as described in the Results of Audit section of this report.

We did not review classified information or *Freedom of Information Act* activities at the DHS Privacy Office. In addition, our review did not include privacy related matters pertaining to OIG.

We conducted this audit between April 2019 through April 2020 pursuant to the *Inspector General Act of 1978*, as amended, and according to generally accepted government auditing standards. Those standards require we plan and perform the audit to obtain sufficient, appropriate evidence to provide reasonable basis for our findings and conclusions based on our audit objective. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Appendix B
DHS Comments to the Draft Report

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

Homeland Security

September 30, 2020

MEMORANDUM FOR: Joseph V. Cuffari, Ph.D.
Inspector General

FROM: Dena Kozanas
Chief Privacy Officer

SUBJECT: Management Response to Draft Report: "DHS Privacy Office Needs to Improve Oversight of Department-wide Activities, Programs, and Initiatives" (Project No. 19-041-AUD-PRIV)

Thank you for the opportunity to comment on the draft report. The U.S. Department of Homeland Security (DHS or the Department) Privacy Office appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review from April 2019 to April 2020 and issuing this report.

The DHS Privacy Office is pleased to note OIG's recognition of the Department's comprehensive framework to protect personally identifiable information (PII) handled through department-wide activities, programs, and initiatives, as required by federal law and policy. Through this framework, the Privacy Office assists the Department in accomplishing its mission while embedding and enforcing privacy protections and transparency in all DHS activities. Specifically, all DHS information technology (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 and the requirements of U.S. data privacy and disclosure laws. Further, the Privacy Office's expertise in privacy and disclosure law, in consultation with DHS's Office of the General Counsel, helps inform privacy and disclosure policy development within the Department and, through collaboration, with the rest of the Federal Government. The Privacy Office remains committed to evaluating Department programs, systems, and initiatives for potential privacy impacts, as well as providing mitigation strategies to reduce the privacy impact.

The Privacy Office also understands the importance of conducting proper oversight to ensure the consistent execution of the Department's privacy policies and requirements across DHS and its Components. Consistent with this understanding and following the completion of the OIG's fieldwork for this audit in April 2020, DHS Acting Secretary

Wolf signed Delegation 130001, "Delegation to the Chief Privacy Officer and Chief Freedom of Information Act Officer (Delegation)," on June 2, 2020. This Delegation vests certain authorities of the Secretary of DHS to the Chief Privacy Officer over the management, governance, and oversight of Component privacy activities. Importantly, this Delegation clarifies the Chief Privacy Officer's oversight authority by stating that he/she is responsible for:

> "Providing appropriate oversight, to the extent consistent with 6 U.S.C.142 and other privacy laws applicable to DHS, and consistent with Federal Government privacy requirements, of how the Department and its Components implement federal and DHS privacy laws, policies, and directives issued pursuant to DHS Directive 112-01."

This delegation also clarifies and strengthens the role of the privacy and disclosure programs across the Department and should substantially improve the Privacy Office's ability to resolve the issues identified by this audit.

The draft report contained three recommendations with which the Privacy Office concurs. Attached find our detailed response to each recommendation. DHS previously submitted technical comments under a separate cover for OIG'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.

Attachment

Attachment: Management Response to Recommendations Contained in OIG 19-041-AUD-PRIV

OIG recommended that the DHS Chief Privacy Officer:

Recommendation 1: Develop and implement an automated process to initiate and schedule timely and periodic reviews of Privacy Threshold Analyses and Privacy Impact Assessments consistent with the DHS Privacy Office policy.

Response: Concur. Prior to the initiation of this OIG audit, the DHS Privacy Office identified the need for a new Compliance Tracking System with automated reporting features that track and schedule the timely reviews of privacy compliance documents (i.e., Privacy Threshold Analyses (PTA), Privacy Impact Assessments (PIA), and Systems of Records Notices (SORN)). Accordingly, the DHS Privacy Office began working with the DHS Office of the Chief Information Officer on a new tracking system known as "PRIVCATS," which the Privacy Office launched in October 2019.

The Privacy Office's prior tracking system, Internet Quorum, did not have a way to accurately capture privacy compliance document renewal requirements or expirations. Further, the systems' reporting metrics were difficult to pull and hard to decipher. The new system, PRIVCATS, allows for the Privacy Office to pull privacy compliance documents that are expired or set to expire in 30, 60, or 90-day increments in order to provide appropriate awareness to DHS Component Privacy Offices.

In August 2020, the Privacy Office completed uploading historical PTAs from 2017 to present into the PRIVCATS system. This is an extensive manual process and the Privacy Office is continuing to upload its PTAs from prior to 2017. In addition, all historical DHS PIAs and SORNs were uploaded into the system prior to its launch in October 2019. Below is the DHS Privacy Office's estimated timeline for completion of this recommendation:

- Upload historical PTAs from 2014-2017 into PRIVCATS by September 30, 2021;
- Upload historical PTAs from 2010-2013 into PRIVCATS by March 31, 2022.

Overall Estimated Completion Date (ECD): March 31, 2022

Recommendation 2: Develop, implement, and formally communicate a process to ensure review of all proposed Information Sharing Access Agreements [ISAA] involving personally identifiable information.

3

Response: Concur. When the DHS originally published "DHS Privacy Policy and Compliance" Directive 047-01 and "DHS Privacy Policy and Compliance" Instruction 047-01-001 in 2011, the Privacy Office was in the beginning stages of understanding and building a role for itself in the Department's information sharing process. Since that time, however, the Privacy Office gained a greater knowledge of the size and scope of the Department's ISAAs.

Accordingly, the DHS Privacy Office started to assess and draft revisions to the Chief Privacy Officer's review requirements related to ISAAs in "DHS Privacy Policy and Compliance" Directive 047-01 and "DHS Privacy Policy and Compliance" Instruction 047-01-001. Specifically, as a result of the high volume of ISAAs developed and entered into by the Department, it is not feasible for the DHS Privacy Office to review each agreement. Therefore, the Privacy Office will develop standards for which types of ISAAs need to be reviewed by the Chief Privacy Officer, and which ISAAs may be delegated for review by Component Privacy Officers and/or Privacy Points of Contact (PPOCs). Below is the DHS Privacy Office's estimated timeline for completion:

- Begin revising "DHS Privacy Policy and Compliance" Directive 047-01 and "DHS Privacy Policy and Compliance" Instruction 047-01-001 by September 30, 2020;
- Begin formal clearance of the Directive and Instruction by January 29, 2021; and
- Publish updated versions of the documents by August 31, 2021.

Overall ECD: August 31, 2021.

Recommendation 3: Develop and implement a process to monitor the completion of mandatory annual privacy training.

Response: Concur. "DHS Privacy Policy and Compliance" Instruction 047-01-001 requires that, "All DHS employees and contractors complete annual online privacy training developed by the Chief Privacy Officer or by Component Privacy Officers or PPOCs in consultation with the Chief Privacy Officer." However, the DHS Privacy Office does not have access to individual Component Learning Management Systems to track mandatory annual privacy training across the DHS enterprise. Further, the Privacy Office identified several DHS Components with differing required completion dates for their annual privacy training, which makes tracking and reporting more difficult at the Headquarters level.

Regardless of these challenges, however, the DHS Privacy Office agrees that a better process to monitor the completion of mandatory annual privacy training is necessary. Therefore, the DHS Privacy Office will work with the DHS Office of Chief Human Capital Officer (OCHCO) to develop a technical solution that ensures the DHS Privacy Office receives its necessary training statistics on mandatory annual privacy training.

4

The DHS Privacy Office will also consult with the DHS Privacy Council, compromised of DHS Component Privacy Officers and PPOCs, to identify potential interim solutions, while the technical solution is developed with OCHCO.

ECD: April 30, 2021.

5

Appendix C
Examples of Previously Issued Privacy Reports

DHS OIG

- *FEMA Did Not Safeguard Disaster Survivors' Sensitive Personally Identifiable Information* (REDACTED) (OIG 19-32) March 2019
- *CBP Has Not Ensured Safeguards for Data Collected Using Unmanned Aircraft Systems* (OIG 18-79) September 2018
- *Office of Health Affairs Has Not Implemented an Effective Privacy Management Program* (OIG 18-20) November 2017
- *USSS Faces Challenges Protecting Sensitive Case Management Systems and Data* (OIG 17-01) October 2016
- *CBP's Office of Professional Responsibility's Privacy Policies and Practices* (OIG-16-123) August 2016
- *United States Coast Guard Safeguards For Protected Health Information Need Improvement* (OIG-15-87) May 2015
- *Federal Emergency Management Agency Privacy Stewardship* (OIG 13-87) May 2013
- *U.S. Customs and Border Protection Privacy Stewardship* (OIG-12-78) April 2012
- *U.S. Citizenship and Immigration Services Privacy Stewardship* (OIG-11-85) May 2011
- *Immigration and Customs Enforcement Privacy Stewardship* (OIG-10-100) July 2010
- *Transportation Security Administration Privacy Stewardship* (OIG-09-97) August 2009

U.S. Government Accountability Office

- *Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach* (GAO 18-559) August 2018
- *DHS Needs to Continue to Advance Initiatives to Protect Federal Systems* (GAO 17-518T) March 2018
- *Immigration Status Verification For Benefits; Actions Needed to Improve Effectiveness and Oversight* (GAO 17-204) March 2017
- *DHS's National Integration Center Generally Performs Required Functions but Needs to Evaluate Its Activities More Completely* (GAO 17-163) February 2017
- *Federal Agencies Need to Better Protect Sensitive Data* (GAO-16-194T) November 2015
- *TSA Could Take Additional Steps to Strengthen Privacy Oversight Mechanisms* (GAO 14-647) September 2014
- *Secure Flight; Additional Actions Needed to Determine Program Effectiveness and Strengthen Privacy Oversight Mechanisms* (GAO 14-796T) September 2014
- *DHS Privacy Office Has Made Progress but Faces Continuing Challenges* (GAO 07-1024T) July 2007

Appendix D
Annual Privacy Awareness Training Completion Rates for DHS Employees and Contractors

2019 Annual Privacy Awareness Training Completion Rates				
Component	Number Assigned	Number Completed	Number Not Completed	Percent Not Completed
Headquarters	9,493	4,648	4,845	51%
CBP	67,645	63,612	4,033	6%
FEMA	19,981	12,689	7,292	36%
ICE	25,126	21,133	3,993	16%
TSA	65,070	62,787	2,283	4%
Coast Guard	55,937	48,636	7,301	13%
USCIS	27,942	26,265	1,677	6%
Secret Service	6,498	5,725	773	12%
Total	**277,692**	**245,495**	**32,197**	**12%**

2018 Annual Privacy Awareness Training Completion Rates				
Component	Number Assigned	Number Completed	Number Not Completed	Percent Not Completed
Headquarters	9,177	4,711	4,466	49%
CBP	61,290	51,977	9,313	15%
FEMA	20,040	5,775	14,265	71%
ICE	26,726	23,191	3,535	13%
TSA	55,455	50,165	5,290	10%
Coast Guard	55,740	49,159	6,581	12%
USCIS	26,668	23,364	3,304	12%
Secret Service	6,705	5,736	969	14%
Total	**261,801**	**214,078**	**47,723**	**18%**

2017 Annual Privacy Awareness Training Completion Rates				
Component	Number Assigned	Number Completed	Number Not Completed	Percent Not Completed
Headquarters	8,470	3,620	4,850	57%
CBP	57,391	48,175	9,216	16%
FEMA	17,751	5,004	12,747	72%
ICE	22,903	20,995	1,908	8%
TSA	48,212	44,469	3,743	8%
Coast Guard	54,665	46,292	8,373	15%
USCIS	25,576	21,928	3,648	14%
Secret Service	No Data	No Data	No Data	No Data
Total	**234,968**	**190,483**	**44,485**	**19%**

Appendix E
Office of Audits, Major Contributors to This Report

Richard Harsche, ATP Audit Director
Jason Kim, Audit Manager
Peter Christopher, Audit Manager
Juan Santana, Auditor in Charge
Vera Cropp, Program Analyst
Rolando Chavez, Auditor
Deborah Mouton-Miller, Communications Analyst
Mark Lonetto, Independent Reference Reviewer

Appendix F
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chiefs of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Under Secretary, Office of Strategy, Policy, and Plans
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

Additional Information and Copies

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.
Follow us on Twitter at: @dhsoig.

OIG Hotline

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive, SW
Washington, DC 20528-0305