Privacy Office

Fiscal Year 2021 Semiannual Report to Congress

Covering the period October 1, 2020 – March 31, 2021

December 21, 2021

FOREWORD

December 21, 2021

I am pleased to present the *U.S. Department of Homeland Security (DHS or Department) Privacy Office's Fiscal Year 2021 Semiannual Report to Congress*, covering the period October 1, 2020 – March 31, 2021.[1]

Highlights

During the reporting period, the DHS Privacy Office:

- Completed 1,167 privacy reviews, including:
  - 871 Privacy Threshold Analyses;
  - 21 Privacy Impact Assessments; and
  - 19 System of Records Notices and associated Privacy Act Exemptions.
- Published the following congressional reports:
  - 2019 DHS Privacy Office Annual Data Mining Report to Congress

About the DHS Privacy Office

The DHS Chief Privacy Officer is the first statutorily mandated Chief Privacy Officer in the federal government. Section 222 of the *Homeland Security Act of 2002* charges the DHS Chief Privacy Officer with ensuring that privacy protections are integrated into all DHS programs, policies, and procedures. The DHS Privacy Office's mission is to sustain privacy protections and to promote transparency in government operations while achieving the mission of the Department. The Chief Privacy Officer serves as the principal advisor to the DHS Secretary on privacy policy and establishes privacy policy for the Department.

The *Privacy Act of 1974* (Privacy Act), as amended, the *Freedom of Information Act* (FOIA), and the *E-Government Act of 2002* require DHS to be transparent in its operations and use of information relating to individuals. The DHS Privacy Office centralizes FOIA and Privacy Act operations to provide policy and programmatic oversight and to support implementation across the Department. The DHS Privacy Office undertakes these statutory and policy-based responsibilities in collaboration with DHS Component privacy[2] and FOIA officers, privacy points of contact, and program offices to ensure that all privacy and disclosure issues are afforded the appropriate level of review and expertise.

[1] Pursuant to the Intelligence Authorization Act for Fiscal Year 2014, Pub. L. No. 113-126 (July 7, 2014), the reporting period was changed from quarterly to semiannually. 42 U.S.C. § 2000ee-1 (2014), Pub. L. No. 113-126, Title III, § 329(b)(4), 128 Stat. 1406 (2014). The DHS Privacy Office semiannual reports cover the following time periods: April – September and October – March.

[2] DHS Components have a Privacy Officer and other DHS offices have a Privacy Point of Contact. A complete list can be found here: http://www.dhs.gov/privacy-office-contacts.

Pursuant to congressional notification requirements, this report is provided to the following Members of Congress:

The Honorable Kamala Harris
President, U.S. Senate

The Honorable Nancy Pelosi
Speaker, U.S. House of Representatives

The Honorable Gary C. Peters
Chairman, U.S. Senate Committee on Homeland Security and Governmental Affairs

The Honorable Rob Portman
Ranking Member, U.S. Senate Committee on Homeland Security and Governmental Affairs

The Honorable Dick Durbin
Chairman, U.S. Senate Committee on the Judiciary

The Honorable Chuck Grassley
Ranking Member, U.S. Senate Committee on the Judiciary

The Honorable Mark Warner
Chairman, U.S. Senate Select Committee on Intelligence

The Honorable Marco Rubio
Vice Chairman, U.S. Senate Select Committee on Intelligence

The Honorable Bennie G. Thompson
Chairman, U.S. House of Representatives Committee on Homeland Security

The Honorable John Katko
Ranking Member, U.S. House of Representatives Committee on Homeland Security

The Honorable Carolyn Maloney
Chairwoman, Acting, U.S. House of Representatives Committee on Oversight and Reform

The Honorable James Comer
Ranking Member, U.S. House of Representatives Committee on Oversight and Reform

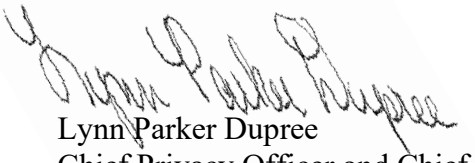
The Honorable Jerrold Nadler
Chairman, U.S. House of Representatives Committee on the Judiciary

The Honorable Jim Jordan
Ranking Member, U.S. House of Representatives Committee on the Judiciary

The Honorable Adam Schiff
Chairman, U.S. House of Representatives Permanent Select Committee on Intelligence

The Honorable Devin Nunes
Ranking Member, U.S. House of Representatives Permanent Select Committee on Intelligence

Sincerely,



Lynn Parker Dupree
Chief Privacy Officer and Chief FOIA Officer
U.S. Department of Homeland Security

DHS Privacy Office
Fiscal Year 2021
Semiannual Report to Congress

Table of Contents

LEGISLATIVE LANGUAGE

Section 803 of the *Implementing Recommendations of the 9/11 Commission Act of 2007,*[3] as amended, sets forth the following requirements:

"(f) Periodic Reports-

(1) In General –

The privacy officers and civil liberties officers of each department, agency, or element referred to or described in subsection (a) or (b) shall periodically, but not less than semiannually, submit a report on the activities of such officers—

(A)(i) to the appropriate committees of Congress, including the Committee on the Judiciary of the Senate, the Committee on the Judiciary of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Oversight and Government Reform of the House of Representatives, the Select Committee on Intelligence of the Senate, and the Permanent Select Committee on Intelligence of the House of Representatives;

(ii) to the head of such department, agency, or element; and

(iii) to the Privacy and Civil Liberties Oversight Board; and

(B) which shall be in unclassified form to the greatest extent possible, with a classified annex where necessary.

(2) Contents –

Each report submitted under paragraph (1) shall include information on the discharge of each of the functions of the officer concerned, including—

(A) information on the number and types of reviews undertaken;

(B) the type of advice provided and the response given to such advice;

(C) the number and nature of the complaints received by the department, agency, or element concerned for alleged violations; and

(D) a summary of the disposition of such complaints, the reviews and inquiries conducted, and the impact of the activities of such officer."

[3] 42 U.S.C. § 2000ee-1(f).

I. PRIVACY REVIEWS

The DHS Privacy Office reviews and evaluates Department programs, systems, and initiatives that collect personally identifiable information (PII) or otherwise have a privacy impact and provides mitigation strategies to reduce the privacy impact. For purposes of this report, privacy reviews include the following:

1. Privacy Threshold Analyses, as required by *DHS Privacy Policy and Compliance Directive 047-01*;
2. Privacy Impact Assessments, as required under the *E-Government Act of 2002,*[4] the *Homeland Security Act of 2002*,[5] and DHS policy;
3. System of Records Notices as required under the *Privacy Act of 1974*, as amended, and any associated Final Rules for Privacy Act exemptions;[6]
4. Privacy Act Statements, as required under the Privacy Act,[7] to provide notice to individuals at the point of collection;
5. Computer Matching Agreements, as required under the Privacy Act;[8]
6. Data Mining Reports, as required by Section 804 of the *9/11 Commission Act of 2007*;[9]
7. Privacy Compliance Reviews, per the authority granted to the Chief Privacy Officer by the *Homeland Security Act of 2002*;[10]
8. Privacy reviews of IT and program budget requests, including Office of Management and Budget (OMB) Exhibit 300s and Enterprise Architecture Alignment Requests through the DHS Enterprise Architecture Board;
9. Information Technology Acquisition Reviews;[11] and
10. Other privacy reviews at the discretion of the Chief Privacy Officer.

---

[4] 44 U.S.C. § 3501 note. *See also* OMB Memorandum, M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (Sept. 26, 2003), *available at*:https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2003/m03_22.pdf.

[5] 6 U.S.C. § 142.

[6] 5 U.S.C. §§ 552a(e)(4), (j), (k). *See also* OMB Circular No. A-108, "Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act," 81 Fed. Reg. 94424 (Dec. 23, 2016), available at: https://www.gpo.gov/fdsys/pkg/FR-2016-12-23/pdf/2016-30901.pdf.

[7] 5 U.S.C. § 552a(e)(3).

[8] 5 U.S.C. § 552a(o)-(u).

[9] 42 U.S.C. § 2000ee-3.

[10] The Chief Privacy Officer and DHS Privacy Office exercise its authority under Section 222 of the Homeland Security Act (6 U.S.C. § 142) to assure that technologies sustain and do not erode privacy protections through the conduct of Privacy Compliance Reviews. Consistent with the Privacy Office's unique position as both an advisor and oversight body for the Department's privacy sensitive programs and systems, the Privacy Compliance Review is designed as a constructive mechanism to improve a program's ability to comply with assurances made in existing privacy compliance documentation.

[11] Section 208 of the E-Government Act requires that agencies conduct a privacy impact assessment before procuring information technology (IT) that collects, maintains, or disseminates information that is in an identifiable form. DHS meets this requirement in part by participating in the Information Technology Acquisition Review (ITAR) process. The DHS Privacy Office reviews these ITAR requests to determine if the IT acquisitions require a new privacy impact assessment to identify and mitigate privacy risks or if they are covered by an existing DHS privacy impact assessment. In addition, the DHS Privacy Office reviews ITAR requests to ensure that appropriate language to safeguard personally identifiable information (PII) and Sensitive PII is included in new and existing contracts and solicitations that have a high risk of unauthorized access to, or disclosure of, sensitive information.

Table I Privacy Reviews Completed: ***October 1, 2020 - March 31, 2021***	
Type of Review	***Number of Reviews***
Privacy Threshold Analyses	871
Privacy Impact Assessments	21
System of Records Notices and associated Privacy Act Exemptions	19
Privacy Act (e)(3) Statements[12]	79
Computer Matching Agreements[13]	3
Data Mining Reports	1
Privacy Compliance Reviews	0
Privacy Reviews of IT and Program Budget Requests[14]	0
Information Technology Acquisition Reviews[15] (ITAR)	173
Other Privacy Reviews	0
Total Reviews	***1,167***

[12] This total does not include all Components; several are permitted by the DHS Privacy Office to review and approve their own Privacy Act statements.
[13] Computer Matching Agreements are typically renewed or re-established.
[14] The Chief Information Officer prepares an annual privacy score as part of its Office of Management and Budget Exhibit 300 reporting. Reviews for this category are reported only during the second semiannual reporting period.
[15] The DHS Privacy Office began conducting ITAR reviews in January 2016.

Privacy Impact Assessments

The Privacy Impact Assessment process is one of the Department's key mechanisms to ensure that DHS programs and technologies sustain privacy protections. In addition to completing privacy impact assessments for new systems and projects, programs, pilots, or information-sharing arrangements not currently subject to a privacy impact assessment, the Department also conducts a triennial review of existing privacy impact assessments to assess and confirm that systems still operate within original parameters. After the triennial review, the Department updates any previously published privacy impact assessments, as appropriate, to inform the public it has completed a review of affected systems.

As of March 31, 2021, 99 percent of the Department's *Federal Information Security Modernization Act* systems requiring a privacy impact assessment had a current privacy impact assessment. During the reporting period, the Office published 21 privacy impact assessments: 16 new and 5 updated.

All published DHS privacy impact assessments are available on the DHS Privacy Office website, www.dhs.gov/privacy.[16]

Below is a summary of significant privacy impact assessments published during the reporting period, along with a hyperlink to the full text. A complete list of privacy impact assessments published during the reporting period can be found in the Appendix.

New Privacy Impact Assessments

DHS/USCIS/PIA-084 ATLAS *(October 30, 2020)*

U.S. Citizenship and Immigration Services (USCIS) developed ATLAS (not an acronym) to automate, streamline, and support accurate exchange of data among USCIS, DHS, and non-DHS systems used to support biometric and biographic-based screening and vetting of immigration requests. ATLAS is used as both an automated check service platform and rule-based screening platform for USCIS. This privacy impact assessment evaluates privacy risks and mitigations associated with ATLAS.

DHS/CBP/PIA-066 CBP Support of CDC for Public Health Contact Tracing *(December 15, 2020)*

U.S. Customs and Border Protection (CBP) assists the Department of Health and Human Services, Centers for Disease Control and Prevention (CDC) with its public health response efforts. CBP has historically transmitted certain biographic information from travelers traveling to the United States from foreign locations to the CDC, upon the CDC's request, to support the CDC's efforts to contact individuals who may have been exposed to communicable diseases during their travels. CBP's support of the CDC's public health response efforts has expanded during the COVID-19 pandemic. CBP published this privacy impact assessment to document its provision of public health emergency response related PII to the CDC.

DHS/CISA/PIA-036 Chemical Facility Anti-Terrorism Standards Program Suspicious Activity Reports *(December 16, 2020)*

The Cybersecurity and Infrastructure Security Agency (CISA) Infrastructure Security Division (ISD) Chemical Security Subdivision, hereafter referred to as Chemical Security, receives notification of security incidents at high-risk chemical facilities. This privacy impact assessment describes the incident and suspicious-activity reporting actions previously performed by CISA's legacy National Infrastructure Coordinating Center and now performed by Chemical Security. This privacy impact assessment outlines the PII CISA routinely receives when evaluating information about security

[16] Privacy impact assessments are unpublished when the subject matter is Law Enforcement Sensitive or involves a National Security System. Unpublished privacy impact assessment is on file with the DHS Privacy Office.

incidents and their potential nexus to terrorism and replaces the DHS/NPPD/PIA-017 NICC Suspicious Activity Report (SAR) Privacy Impact Assessment.

DHS/ALL/PIA-088 Preventing Infectious Disease at DHS Facilities During Declared Public Health Emergencies *(December 21, 2020)*
DHS issued to Components discretionary guidance designed to prevent the spread of infectious disease or illness among its workforce in the event of a declared public health emergency. These processes include workforce accountability tracking, basic health screening of individuals attempting to enter DHS facilities, laboratory testing of personnel and visitors scheduled to occupy or visit certain DHS facilities, and contact tracing to identify members of the DHS workforce or visitors who might have been exposed while at a DHS worksite. DHS conducted this Privacy Impact Assessment because some of these processes involve the collection and use of PII.

DHS/ALL/PIA-089 DHS International Biometric Interoperability Initiative for the Visa Waiver Program *(January 7, 2021)*
The Visa Waiver Program, administered by DHS in consultation with the Department of State, permits citizens of designated countries to travel to the United States for business or tourism for stays of up to 90 days without a visa. The eligibility requirements for a country's designation in the Visa Waiver Program are defined in Section 217 of the Immigration and Nationality Act (INA) (including as amended most recently by the Visa Waiver Program Improvement and Terrorist Travel Prevention Act of 2015). A requirement of the program is that any country seeking to participate must enter into and implement an agreement with the United States to share information regarding whether citizens and nationals of that country traveling to the United States represent a threat to the security or welfare of the United States or its citizens.

To implement this program requirement in a manner consistent with law, Presidential Memoranda, and DHS's increasing requirements for mission-based traveler screening, DHS determined all countries in the Visa Waiver Program and those aspiring to join must allow DHS and State to compare the fingerprints of travelers and immigration-benefit applicants against appropriate records, including identity, criminal, and terrorist records, for purposes of border security, immigration, and traveler screening. This enhancement to Visa Waiver Program screening capabilities enables DHS to better identify individuals who pose a threat to the security or welfare of the United States. This Privacy Impact Assessment considers privacy risks and applicable mitigation strategies associated with implementing Departmental policy.

Updated Privacy Impact Assessments

DHS/TSA/PIA-046(c) Travel Document Checker Automation Using Facial Identification *(January 28, 2021)*
The DHS Transportation Security Administration (TSA) enhanced the identity verification of passengers using facial identification technology at airports. In previous proofs of concept, TSA used a Credential Authentication Technology device equipped with a camera to validate that the identity document presented by the passenger was authentic and to compare the passenger's live facial image against the image from the passenger's identity document. TSA conducted a new proof of concept at Detroit Metropolitan Wayne County Airport in cooperation with Delta Airlines. In the new proof of concept, TSA used the CBP Traveler Verification Service to pre-stage a gallery of passenger photographs for certain TSA PreCheck® and CBP Global Entry passengers. These passengers' opt-in during the check-in process to have their image captured and use their photograph(s) already on file with DHS for identity verification at TSA checkpoints. Only CBP Global Entry passengers and TSA PreCheck passengers who have a U.S. passport were eligible to participate in this proof of concept.

Data from the proof of concept is shared with the DHS Science and Technology Directorate (S&T) for subsequent qualitative and quantitative analysis. This Privacy Impact Assessment Update was conducted pursuant to Section 222 of the Homeland Security Act to address privacy risks caused by connecting the CBP Traveler Verification Service to the TSA checkpoint identity verification system.

DHS/CISA/PIA-030(a) Continuous Diagnostics and Mitigation (*December 19, 2019)*
CISA's Cybersecurity Division developed the Continuous Diagnostics and Mitigation program to support government-wide and agency-specific efforts to implement adequate, risk-based, and cost-effective cybersecurity. The Continuous Diagnostics and Mitigation program provides continuous monitoring, diagnostics, and mitigation tools and services to strengthen the security posture of participating federal civilian departments and agencies' systems and networks. The Continuous Diagnostics and Mitigation program establishes a suite of capabilities that enables network security officials and administrators to know the state of their respective networks at any given time, informs Chief Information Officers and Chief Information Security Officers on the relative risk of threats, and makes it possible for government personnel to identify and mitigate vulnerabilities.

This Privacy Impact Assessment Update assesses privacy risks related to the Continuous Diagnostics and Mitigation program Shared Service Platform, which makes the Continuous Diagnostics and Mitigation program capabilities available for use by non-Chief Financial Officer Act agencies. The Shared Service Platform is provided to non-Chief Financial Officer Act agencies using a third-party contractor to CISA that connects the agency's network(s) to the platform. Additionally, this Privacy Impact Assessment Update examines the non-Chief Financial Officer Agency-Wide Adaptive Risk Enumeration capability, which allows participating agencies to better assess and prioritize cybersecurity risks by assigning a risk score to agency vulnerabilities.

System of Records Notices

The Department publishes System of Records Notices consistent with requirements outlined in the *Privacy Act of 1974,* as amended.[17] The Department conducts assessments to ensure that: all System of Records Notices remain accurate, up-to-date, and appropriately scoped; all System of Records Notices are published in the *Federal Register*; and all new System of Records Notices and all significant changes to System of Records Notices are reported to OMB and Congress.

As of March 31, 2021, 100 percent of the Department's Privacy Act systems of records had an up-to-date System of Records Notice published in the *Federal Register*. During the reporting period, the Privacy Office published 13 System of Records Notices: three new, ten updated, and six Privacy Act rulemakings.[18]

Below is a summary of significant System of Records Notices published during the reporting period, along with a hyperlink to the full text in the *Federal Register.* All published DHS System of Records Notices and Privacy Act rulemakings are available on the DHS Privacy Office website, https://www.dhs.gov/privacy. A complete list of all System of Records Notices published during the reporting period can be found in the Appendix.

New System of Records Notices

DHS/ALL-046 Counterintelligence Program

The purpose of this system is to collect, store, and maintain records related to, and in furtherance of, counterintelligence collections and activities of the DHS Counterintelligence Program. DHS uses this system to conduct administrative inquiries to identify, analyze, and neutralize foreign intelligence threats to DHS personnel, facilities, equipment, networks, information, and activities; report on foreign contacts and travel, including briefings and debriefings; conduct counterintelligence investigative activities and produce intelligence on foreign intelligence entities; provide counterintelligence awareness training; and other activities relating to the DHS Counterintelligence Program's responsibilities. *(85 Fed. Reg. 80800, December 14, 2020).*

[17] 5 U.S.C. §§ 552a(e)(4), (j), (k). *See also* OMB Circular No. A-108, "Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act," 81 Fed. Reg. 94424 (Dec. 23, 2016), available at: https://www.gpo.gov/fdsys/pkg/FR-2016-12-23/pdf/2016-30901.pdf.

[18] These System of Records Notices can be all found in the Federal Register at the below citations:

- DHS/ALL-023 Department of Homeland Security Personnel Security Management, October 13, 2020, 85 FR 64511
- DHS/ALL-046 Counterintelligence Program System of Records, December 14, 2020, 85 FR 80800
- DHS/ALL-047 Records Related to DHS Personnel, Long-Term Trainees, Contractors, Mission Support Individuals, and Visitors During a Declared Public Health Emergency System of Records, December 11, 2020, 85 FR 80127
- DHS/CBP-018 Customs Trade Partnership Against Terrorism (CTPAT), March 22, 2021, 86 FR 15241
- DHS/CBP-024 Intelligence Records System (CIRS) System of Records, December 14, 2020, 85 FR 80806
- DHS/FEMA-014 Hazard Mitigation Planning and Flood Mapping Products and Services Records System of Records, January 11, 2021, 86 FR 1988
- DHS/FEMA-015 Fraud Investigations System of Records, March 22, 2021, 86 FR 15237
- DHS/ICE-004 Bond Management Information System (BMIS), October 13, 2020, 85 FR 64515
- DHS/ICE-009 External Investigations, November 20, 2020, 85 FR 74362
- DHS/ICE-018 Analytical Records, March 22, 2021, 86 FR 15246
- DHS/USCG-061 Maritime Analytic Support System (MASS), November 23, 2020, 85 FR 74742
- DHS/USSS-001 Criminal Investigation Information October 13, 2020, 85 FR 64523
- DHS/USSS-004 Protection Information System October 13, 2020, 85 FR 64519

DHS/FEMA-015 Fraud Investigations System
The purpose of this system is to collect, maintain, and share records related to fraud investigations conducted by the Federal Emergency Management Agency (FEMA) Fraud and Internal Investigations Division. It allows FEMA to conduct necessary investigations to safeguard and protect federal disaster funds and/or benefits from fraud against the United States. *(86 Fed. Reg. 15237, March 22, 2021).*

DHS/ICE-018 Analytical Records
This new agency-wide system of records notice covers records maintained by U.S. Immigration and Customs Enforcement (ICE) to allow personnel to search, aggregate, and visualize large volumes of information to enforce criminal, civil, and administrative laws under ICE's jurisdiction. *(86 Fed. Reg. 15247, March 22, 2021).*

Updated System of Records Notices

DHS/USSS-001 Criminal Investigation Information System
The purpose of this system is to collect and maintain criminal records related to individuals investigated by DHS United States Secret Service (USSS) in connection with USSS's criminal law enforcement functions, including investigating counterfeiting offenses, financial institution fraud, computer and telecommunications fraud, false identification documents, access device fraud, advance fee fraud, and electronic funds transfer fraud. (*Reg. 64523, October 13, 2020).*

DHS/USCG-061 Maritime Awareness Global Network (MAGNET)
The purpose of this system is to enhance U.S. Coast Guard (USCG) capabilities by developing a total picture of the maritime environment and the people, places, and things it affects. Enhancements of this picture effectively promote successful execution of the Coast Guard's statutory missions of Port, Waterways, and Coastal Security; Drug Interdiction; Aid to Maritime Navigation; Search and Rescue Operations; Protection of Living Marine Resources; Ensuring Marine Safety; Defense Readiness; Migrant Interdiction; Marine Environmental Protection; Ice Operations; and Law Enforcement. *(85 Fed. Reg. 74742, November 23, 2020).*

DHS/ALL-047 Records Related to DHS Personnel, Long-Term Trainees, Contractors, and Visitors During a Declared Public Health Emergency System
The purpose of this system is to maintain records to protect the Department's workforce and respond to a declared public health emergency. For instance, DHS may use information collected to conduct contact tracing (i.e., the subsequent identification, monitoring, and support of a confirmed or probable case's close contacts who have been exposed to, and possibly infected with, the disease or illness at or on buildings, grounds, and properties that are owned, leased, or used by DHS); institute preventative testing to permit entry to buildings, grounds, and properties owned, leased, or used by DHS to minimize exposure; and fulfill testing reporting requirements, to the extent permitted by law. *(85 Fed. Reg. 80127, December 11, 2020).*

Privacy Compliance Reviews

The Privacy Office serves as both an advisor and oversight body for the Department's privacy-sensitive programs and systems. The Privacy Compliance Review was designed as a collaborative effort to help improve a program's ability to comply with existing privacy compliance documentation, including Privacy Impact Assessments, System of Records Notices, and/or formal agreements such as Memoranda of Understanding or Memoranda of Agreements. DHS Privacy Policy Instruction 047-01-004 for Privacy Compliance Reviews implements DHS Directive 047-01, "Privacy Policy and Compliance," regarding Component Heads' responsibility to assist the Chief Privacy Officer in reviewing Component activities to ensure privacy protections are fully integrated into Component operations.

A Privacy Compliance Review may result in a public report or internal recommendations, depending on the sensitivity of the program under review. The Privacy Office tracks implementation of Privacy Compliance Review recommendations based on supporting evidence provided by the Component Privacy Office and/or Program reviewed. A list of Privacy Compliance Review recommendations not yet implemented are listed on the Privacy Office website, www.dhs.gov/privacy, under Privacy Oversight, along with all public-facing Privacy Compliance Reviews.

- Two Privacy Compliance Reviews were launched during this reporting period: (1) U.S. Citizenship & Immigration Services Fraud Detection & National Security Directorate and (2) Office of Biometric Identity Management Homeland Advanced Recognition Technology.

II. Advice and Responses

This section highlights privacy policy guidance and recommendations provided by the DHS Privacy Office.

Privacy Policy Initiatives

Privacy Policy Assessment Project

The DHS Privacy Office continues to evaluate privacy policies,[19] directives, and instructions to ensure that they comply with Departmental requirements, that technical content is updated and accurate, and that policies are in line with updated legislative requirements. Next steps in the multi-phase evaluation include preparing updates to the first set of identified policies, directives, and instructions, and reformatting legacy policies to better facilitate use and reference. Future phases will include implementing processes to conduct interval-based reviews, ascertaining whether current policy inventory addresses DHS Privacy Office operational needs, and developing a formal communications and implementation strategy for new and existing policies.

[19] DHS privacy policies available at: https://www.dhs.gov/privacy-policy-guidance.

III. Training and Outreach

Mandatory Online Training

125,271 DHS personnel completed a mandatory computer-assisted privacy awareness training course entitled, "Privacy at DHS: Protecting Personal Information." This course is required for all personnel when they join the Department, and annually thereafter.

41,785 DHS personnel completed training on the operational use of social media during this reporting period, as required by DHS Directive Instruction Number 110-01-001, Privacy Policy for Operational Use of Social Media, and applicable DHS Privacy Office-adjudicated Component Social Media Operational Use Template(s).

Classroom Training

5,349 DHS personnel attended instructor-led privacy training courses, including the following for which the DHS Privacy Office either sponsored or provided a trainer:

- ***FOIA Training***: This periodic training is tailored to FOIA staff throughout the Department responsible for processing FOIA requests.
    - **March 2021 - Sunshine Week FOIA Training.** The DHS Privacy Office provided more than 400 FOIA professionals with training during the 2021 Sunshine Week FOIA Training Summit. The Department of Treasury co-hosted the event. Sunshine Week training covered several critical topics, including working with requesters to narrow broad requests and what to expect in FOIA litigation. The DHS Privacy Office shared a recording of the event afterwards.
- ***International Attaché Training***: The Department's International Pre-Deployment training module is a week-long course designed to prepare DHS employees who serve as DHS attachés at U.S. embassies worldwide by providing them with basic information on each Component's international activities. During the training, the Privacy Office provides a session on international privacy policy to raise awareness among new attachés of the potential impact global privacy policies may have on DHS operations. Due to the pandemic, no in-person classes were held this period and a session on international privacy was not included in the virtual offering. When in-person classes resume, training will include the privacy session.
- ***New Employee Orientation***: The DHS Privacy Office provides privacy training as part of the Department's bi-weekly orientation session for all new headquarters employees. Many Component Privacy Officers also offer privacy training for new employees in their respective Components. In addition, the DHS Privacy Office provides monthly privacy training as part of the two-day course, *DHS 101*, required for all new and existing headquarters staff.
- ***Privacy Briefings for Headquarters Staff*:** The DHS Privacy Office provides classroom privacy awareness training to Headquarters staff with an emphasis on identifying and resolving data vulnerabilities involving PII.
- ***Role-Based Training***: The DHS Privacy Office trains DHS Contracting Officers and Contracting Officers' Representatives on how to embed privacy protections into contracts. Acquisition management staff, which includes the Heads of the Contracting Activities, Component Acquisition Executives, and Component acquisition policy representatives, received training.
- ***DHS Privacy Office Boot Camp***: The DHS Privacy Office periodically trains new Component privacy staff compliance best practices, including how to draft Privacy Threshold Analyses, Privacy Impact Assessments, and System of Records Notices.

- ***Reports Officer Course*:** The DHS Privacy Office provides privacy training to DHS Intelligence Enterprise reports officers who prepare intelligence reports.
- ***Raw Intelligence Release Authority Course:*** The DHS Privacy Office provides instruction to members of the DHS Intelligence Enterprise who seek the authority to approve raw intelligence for dissemination outside the federal government.
- ***Finished Intelligence Release Authority Course:*** The DHS Privacy Office provides instruction to members of the DHS Intelligence Enterprise who seek the authority to approve finished intelligence products for dissemination outside the federal government.
- ***Security Specialist Course*:** The DHS Privacy Office provides privacy training every six weeks to participants of this week-long interagency training program.

DHS Component Privacy Office Training and Outreach

This section features proactive steps taken by DHS Component Privacy Offices to educate and inform DHS staff on privacy law and policy.

Cybersecurity and Infrastructure Security Agency (CISA)

- **311** CISA personnel attended instructor-led privacy training courses.
    - On June 22 and 23, 2021, privacy analysts from the CISA Office of the Chief Privacy Officer conducted a privacy training to 44 individuals across CISA regarding privacy reviews in the Information Technology Acquisition Review process.
    - The CISA Office of the Chief Privacy Officer provided a privacy briefing during New-Employee Orientation to a total of 267 new CISA employees across all divisions. (These attendees are captured in the grand total above: CISA personnel attended instructor-led privacy training courses.)
- **48** CISA personnel and contractors completed training on the operational use of social media, as required by the DHS Privacy Policy for Operational Use of Social Media. Audiences included personnel supporting CISA's Integrated Operations Division, CISA Central, the CISA Executive Briefing team, and CISA Regional Operations teams.
- CISA's Office of the Chief Privacy Officer published two issues (December and March) of the quarterly privacy newsletter, *CISA Privacy Update.* The newsletter is distributed CISA-wide and posted on CISA's Office of Chief Privacy Officer intranet page.

Federal Emergency Management Agency (FEMA)

- **335** FEMA personnel completed instructor-led privacy training courses.
- **7,709** FEMA personnel completed the mandatory annual computer-assisted privacy awareness training course *Privacy at DHS: Protecting Personal Information*.
- **30** FEMA personnel completed training on the operational use of social media during the reporting period as required by DHS Directive Instruction Number 110-01-001, *Privacy Policy for Operational Use of Social Media*.

Federal Law Enforcement Training Centers (FLETC)

- **493** FLETC personnel completed the mandatory annual computer-assisted privacy awareness training course: *Privacy at DHS: Protecting Personal Information*.

Intelligence and Analysis (I&A)

- **648** I&A personnel completed instructor-led privacy training courses.
    - I&A's primary form of privacy-focused training is delivered through the mandatory annual training requirement on I&A's Attorney General-approved Intelligence Oversight (IO) Guidelines, which contain a number of requirements and restrictions on the handling of PII, particularly regarding U.S. persons. Intelligence Oversight training is provided by I&A's Privacy and Intelligence Oversight Branch.

- 355 I&A personnel received a privacy-focused training component as part of a larger training course offered through the Intelligence Training Academy.

- 169 I&A personnel received mandatory Intelligence Oversight training either as part of new-employee orientation or as part of a targeted effort by I&A's Privacy and Intelligence Oversight Branch to address Intelligence Oversight concerns specific to missions, activities, or subject matters.

- 293 I&A personnel received privacy training during a three-day course on Open-Source Intelligence by the Intelligence Training Academy.

- On October 29-30, 2020, the I&A Privacy and Intelligence Oversight Branch partnered with the Office of General Counsel (OGC) Intelligence Law Division to provide a live, virtual overview of privacy and legal restrictions to I&A's Collection Management Division, which plays a key role in the dissemination of virtually all DHS intelligence products.

Office of the Chief Human Capital Officer (OCHCO)

- **324** OCHCO personnel completed instructor-led privacy training courses.

- **29** OCHCO personnel completed the mandatory annual computer-assisted privacy awareness training course: *Privacy at DHS: Protecting Personal Information*.

Science & Technology Directorate (S&T)

- **372** S&T personnel completed instructor-led privacy training courses.

- The S&T Privacy Office continued to engage with OGC in drafting updated policy guidance for the use of publicly available information in S&T research, development, testing, and evaluation efforts. The S&T Privacy Office also updated specific training and rules of behavior to provide relevant S&T employees.

- The S&T Privacy Office led a discussion of the Privacy Roundtable regarding how S&T's revitalization facilitated cross-collaboration within S&T and DHS Components and how S&T's privacy program is ensuring privacy by design principles. The presentation specifically addressed how the S&T Privacy Office and the S&T Counter-Unmanned Aircraft Systems program work together with partnering DHS Components to ensure the privacy provisions of the Preventing Emerging Threats Act are properly implemented within DHS.

- The S&T Privacy Office provided training to awardees of the Silicon Valley Innovation Program's Preventing Forgery/Counterfeiting Topic Call. The presentation included updated materials tailored specifically for consumption by the private sector blockchain audience. The S&T Privacy Office delivered the presentation as part of a day-long Industry Day meant to educate the awardees on issues that may impact implementation of their innovative technology solutions for preventing forgery and counterfeiting.

- The S&T Privacy Office was featured on the Deconstructing Small Business Innovation Research Webinar Series to provide insight to potential Small Business partners on how the S&T Privacy Office integrates privacy protections into S&T's Small Business Innovation

Research projects. There were 120 attendees for the live virtual presentation, and there have been 279 views of the recording posted to the S&T YouTube channel, as of March 31.

- The S&T Privacy Office provided a briefing to the S&T Office of the Chief Information Officer to discuss the role of Privacy in the development and authorization of IT systems.

- The S&T Privacy Office held a series of discussions with the DHS Compliance Assurance Program Office to provide an overview of privacy practices and principles, with attention to how privacy protections intersect with general protections for human subjects involved in DHS research.

Transportation Security Administration (TSA)

- **27** TSA personnel completed instructor-led privacy training courses.

    - The TSA Privacy Office conducted training for TSA's Information System Security Officers on preparing DHS Privacy Threshold Analyses.

- **48,124** TSA personnel completed the mandatory annual computer-assisted privacy awareness training course: *Privacy at DHS: Protecting Personal Information.*

- The TSA Privacy Office conducted outreach to advocacy groups on TSA use of facial-identity verification technology.

U.S. Citizenship and Immigration Services (USCIS)

- **790** USCIS personnel completed instructor-led privacy awareness training courses.

    - The USCIS Office of Privacy conducted bi-weekly instructor-led privacy awareness trainings for new USCIS Headquarters employees.

    - The USCIS Office of Privacy conducted instructor-led privacy awareness trainings for several USCIS offices and programs to include the Office of Human Capital and Training, the Miami Field Office, the California Service Center, and the National Records Center. These trainings were provided upon request from the offices and in response to internal outreach initiatives.

    - The USCIS Office of Privacy conducted privacy training for 53 Contract Officers and Contract Officer's Representatives on how to complete the Department of Homeland Security Acquisition Manual Appendix G Form from a privacy viewpoint and what items should be included in the service description to allow the USCIS Office of Privacy to make a clear determination on whether the contract should be considered high risk and if privacy compliance documentation is required.

- **4,049** USCIS personnel completed the mandatory annual computer-based privacy awareness training course: *USCIS Privacy Awareness Training*.

- **45** USCIS personnel completed training on operational use of social media during the reporting period, as required by DHS Directive Instruction Number 110-01-001, *Privacy Policy for Operational Use of Social Media*.

- The USCIS Office of Privacy conducted several privacy awareness activities, including:
  - Developing an awareness video on the use of social media to include DHS requirements for operational use of social media;
  - Developing and disseminating a one-page informational document entitled Display of PII and Sensitive PII through Collaboration Tools – Best Practices Guide, March 26, 2021;
  - Developing and disseminating the USCIS Office of Privacy's quarterly newsletter entitled "Privacy Chronicles;"
  - Developing and disseminating a guidance memo entitled Monitoring Our Use of Social Security Numbers, October 14, 2020. This memo serves as a reminder to USCIS personnel of their responsibility to limit use of and to protect full Social Security Numbers;
  - Providing a briefing to the Service Centers Operations Enterprise Collaboration Network and Connect working group on privacy compliance, policy, and data protection. This briefing/discussion also kicked off a working group to address governance, best practices, and policy for SharePoint online due to the migration from traditional Enterprise Collaboration Network on March 31, 2021;
  - Conducting a Q&A session with Service Centers Operations Fraud Detection and National Security leadership from all service centers and HQ Service Centers Operations on March 23, 2021. This Q&A addressed emerging technologies and their effect on data protection for sensitive data, i.e., Special Protected Class, law-enforcement-sensitive data, etc.;
  - Conducting disclosure training for Service Centers Operations Background Check Unit leadership on January 12, 2021. This was a targeted training/discussion with leadership of the Unit. The training/discussion focused on what the Background Check Units can disclose, to whom, how, and how to document the disclosure;
  - Conducting an Information Sharing Agreement briefing on January 6, 2021. This briefing/discussion with the Service Centers Operations Fraud Chief and supervisors talks through the ISA process, which addresses current information-sharing agreements, and specifically how to adjust/update Information Sharing Agreements;
  - Conducting a short instruction session regarding the Service Centers Operations Background Check Referral System on December 16, 2020. The session addressed the privacy compliance process, policy, and Q&A;
  - Providing a tailored briefing (overview) of USCIS privacy-related policies and procedures to the incoming Yakima Field Office Director on January 21, 2021;
  - Conducting multiple Q&A sessions and briefings on the privacy compliance process and data-protection requirements for USCIS system developers and programs, including:
    - The Office of Equal Opportunity and Inclusion, Complaints Resolution Division regarding the development of the Enterprise Adobe AEM File Sharing System Request solution on October 5, 2020;
    - The Office of Security and Integrity Personnel Security Division regarding the LexisNexis Insider Threat Portal on November 16, 2020;
    - The Office of Information Technology system owners regarding requirements for updates to the CAMINO system on November 30, 2020;
    - The International and Refugee Affairs Division, Innovation and Design for Enhanced Adjudication Branch regarding the development of the International and Refugee Affairs Division Global System on December 8, 2020; and
    - The Network Analytics team regarding a new system initiative that involves PII on January 29, 2021.

U.S. Coast Guard (USCG)

- **187** USCG personnel completed instructor-led privacy training courses.

    - The USCG Privacy Office presented training to the bi-Monthly CG Civilian Employee Orientation sessions, which were attended virtually by 183 newcomers. The forum focused on raising awareness of the importance of protecting personal information while assigned to the Department of Homeland Security. Privacy staff distributed and discussed DHS policy outlined in the DHS factsheet titled "How to Safeguard Sensitive PII" and the Coast Guard Cybersecurity Manual, COMDTINST M5500.13 (series).

- **11,991** USCG personnel completed the mandatory annual computer-assisted privacy awareness training course: *Privacy at DHS: Protecting Personal Information*.

- **70** USCG personnel completed training on operational use of social media during the reporting period, as required by DHS Directive Instruction Number 110-01-001, *Privacy Policy for Operational Use of Social Media*.

- The USCG Privacy Office provided flyers emphasizing requirements and instructions for encrypting electronic sensitive information to all Commands remediating incidents involving unauthorized release of un-encrypted or non-password protected PII/sensitive PII.

- The USCG Privacy Office expanded privacy-awareness campaigns service-wide by routinely publishing informative notices on the "Special Notices" page on the Coast Guard Portal, as well as television screens located throughout the St. Elizabeth Campus in Washington, DC. During this reporting period, three notices were published.

U.S. Customs and Border Protection (CBP)

- **668** CBP personnel completed instructor-led privacy training courses.

- **24,746** CBP personnel completed the mandatory annual computer-assisted privacy awareness training course: *Privacy at DHS: Protecting Personal Information*.

- **41,292** CBP personnel completed training on operational use of social media during the reporting period, as required by DHS Directive Instruction Number 110-01-001, *Privacy Policy for Operational Use of Social Media*.

- The CBP Privacy Office continues to drive its outreach and awareness campaigns, despite COVID-19 limitations. During the period, the CBP Privacy Office provided 100% of all instructor-led training virtually through various program offices to include: Atlanta Hartsfield-Jackson International Airport, Office of Acquisitions, Audit Liaisons, Privacy & Diversity Office – Equal Employment Opportunity & Freedom of Information Act Divisions, Office of International Affairs, Office of Finance, and Regulatory Audit – Office of Trade. The trainings ranged from foundational refresher privacy training, privacy compliance training, and information sharing training. The CBP Privacy Office is also an annual participant in the Office of Acquisitions' annual 'brown bag lunch series' training venue to facilitate discussions of privacy inclusion in contract administration, with respect to the Homeland Security Acquisition Regulation clauses and other privacy fundamentals.

- The CBP Privacy Office worked with the Laredo, Texas Sector Leadership to craft a detailed privacy message/reminder, which was disseminated with other pertinent privacy-resource materials

to all Laredo Sector employees to remind, educate, and/or bring awareness to employees of their responsibilities under the Privacy Act of 1974, as amended.

- The CBP Privacy Office disseminated an updated "CBP Safeguarding PII Factsheet" via CBP Central to all employees. CBP Central is a weekly one-stop announcement center for CBP employees. Modifications/updates were made to the Factsheet to capture new areas of concern identified using privacy-incident metrics and to bridge knowledge gaps. Furthermore, the CBP Privacy Office utilized the Agency's Information Display System and main internal webpage to broadcast proactive holiday-, sports-, and season-themed privacy messages and reminders to continue to heighten awareness and expand the privacy footprint throughout the Agency.

U.S. Immigration and Customs Enforcement (ICE)

- **977** ICE personnel completed instructor-led privacy training courses.
  - Approximately 116 ICE personnel completed 12 virtual New-Hire Orientation privacy training sessions.
  - About 38 attendees attended an ICE Fundamentals of Mission Support training session addressing general privacy and records management concepts, as well as an overview of Freedom of Information Act requests and responses, on March 9, 2021.
  - On January 28, 2021, approximately 25 Information System Security Officers attended a training session regarding privacy and information security requirements that are built into the system development lifecycle.
  - In March 2021, nearly 900 Enforcement and Removal Officers attended one of three privacy training sessions. The trainings provided a privacy overview and addressed: protecting PII and sensitive PII; communication strategies, including email protocol when sending to non-DHS-gov networks; special issues highlighted by teleworking status; the use of removal drives; encryption and password protection; and an introduction to the cloud-based online collaboration and sharing solution, HUDDLE.
  - Twenty-seven people attended a privacy training session on Homeland Security Investigations (HSI) Domestic Operations on March 24, 2021.
  - On March 16, 2021, 9 people attended a training on the privacy requirements for social media open-source intelligence tools, which addressed background and authorities, disclosure of PII, disclosure scenarios, information sharing, privacy-incident handling, and included cautionary tales.
  - 180 HSI agents attended a training session on the use of third-party facial recognition services on February 11, 2021.
- **6,379** ICE personnel completed the mandatory annual computer-assisted privacy awareness training course: *Privacy at DHS: Protecting Personal Information*.
- **16** ICE personnel completed training on operational use of social media training during the reporting period as required by DHS Directive Instruction Number 110-01-001, *Privacy Policy for Operational Use of Social Media*.

- On March 10, 2021, the ICE Privacy Officer conducted a discussion on initiatives pertaining to the confidentiality provisions found in 8 U.S.C. § 1367 with the ICE Data Governance Board.

U.S. Secret Service (USSS)

- **99** USSS personnel completed instructor-led privacy training courses.

- **1,156** USSS personnel completed the mandatory annual computer-assisted privacy awareness training course: *Privacy at DHS: Protecting Personal Information*.

- **283** USSS personnel completed training on operational use of social media during the reporting period, as required by DHS Directive Instruction Number 110-01-001, *Privacy Policy for Operational Use of Social Media.*

- In October 2020, a service-wide message was sent to all USSS employees emphasizing privacy awareness and proper handling and safeguarding of PII and sensitive PII in daily activities.

- On January 28, 2021, the USSS Privacy Program posted a digital poster and web banner that were both created and used in recognition of International Data Privacy Day. The digital poster was displayed on all digital kiosks on every floor of the USSS Headquarters building, and the digital banner with a linked Privacy Awareness tip sheet was posted onto the front page of the USSS intranet. This tip sheet provided key points to alert employees, both in Headquarters and in field offices, of ways to safeguard and protect PII and sensitive PII. The poster and banner ran on the digital kiosks and the USSS intranet for the entire week.

- November 2020, the USSS Privacy Program updated the New Employee Orientation Privacy Awareness video segment, which is viewed by all onboarding employees entering the agency. The video briefs new employees on proper safeguarding and protection of PII and sensitive PII, advises employees of when it is necessary to initiate/renew/dispose of a Privacy Threshold Analysis, and further instructs new employees on reporting privacy incidents and complaints.

IV. PRIVACY COMPLAINTS

The DHS Privacy Office is responsible for ensuring that the Department has procedures in place to receive, investigate, respond to, and, when appropriate, provide redress for privacy complaints. As required by Section 803 of the *Implementing Recommendations of the 9/11 Commission Act of 2007*, as amended, the DHS Privacy Office is required to provide semi-annual reports to Congress with the number and nature of the complaints received by the Department for alleged violations, and a summary of the disposition of such complaints, when available.

The DHS Privacy Office reviews and responds to privacy complaints referred by employees throughout the Department, or complaints submitted by other government agencies, the private sector, or the public. DHS Components manage and customize their privacy complaint handling processes to align with their specific missions, and to comply with Department complaint-handling and reporting requirements.

DHS separates privacy complaints into four types:

1. ***Procedure:*** Issues concerning process and procedure, such as consent, collection, and appropriate notice at the time of collection, or notices provided in the *Federal Register*, such as Privacy Act System of Records Notices.
    a. *Example*: An individual alleges that a program violates the Privacy Act or Departmental privacy policies by collecting Social Security numbers without providing proper notice.
2. ***Redress:*** Issues concerning appropriate access (not to include FOIA or Privacy Act requests) or correction to PII held by DHS. Redress also includes privacy-related complaints under the DHS Traveler Redress Inquiry Program (DHS TRIP). See below for more information.
    a. *Example:* An individual reports being misidentified during a credentialing process or during traveler inspection at the border or screening at airports.
3. ***Operational:*** Issues related to general privacy concerns or other concerns that are not addressed in process or redress, but do not pertain to Privacy Act matters.
    a. *Example:* An individual alleges that personal health information was disclosed to a non-supervisor.
    b. *Example:* An individual alleges that physical screening and pat down procedures at airports violate their privacy rights.
4. ***Referred*:** Complaints referred to another federal agency or external entity for handling.
    a. *Example:* An individual submits an inquiry regarding his driver's license or Social Security number.

The DHS Privacy Office reviews redress complaints received by the DHS Traveler Redress Inquiry Program (DHS TRIP) that may have a privacy nexus. DHS TRIP is a single point of contact for individuals who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs—like airports—or crossing U.S. borders. This includes watchlist issues, screening problems at ports of entry, and situations where travelers believe they have been unfairly or incorrectly delayed, denied boarding, or identified for additional screening at our nation's transportation hubs.

The DHS TRIP complaint form includes a privacy check box that reads: *I believe my privacy has been violated because a government agent has exposed or inappropriately shared my personal information.* During the reporting period, there were **479** travelers who marked that box. Upon review, none of the complaints received through TRIP described a privacy violation.

During the reporting period, the Department received **26** privacy complaints outside of the TRIP process.

Privacy Complaints Received by DHS Components and the DHS Traveler Redress Inquiry Program *October 1, 2020 – March 31, 2021*					
Type	**CBP**	**FEMA**	**FPS**	**TSA**	**TOTAL**
Procedure	3	1	1	0	**5**
Redress	0	0	0	0	**0**
Operational	14	0	0	7	**21**
Referred	0	0	0	0	**0**
TOTALS	**17**	**1**	**1**	**7**	**26**

***Narrative examples*:**

CBP

- **Operational:** Members of the public reported that friends and family members were allegedly unduly detained or subjected to extensive questioning. CBP Privacy provided submitters with information regarding Privacy Act restrictions and directions for obtaining and submitting written authorization from a third party to disclose information.

TSA

- **Operational**: A member of the public complained that he had not received a response to an application for a TSA credential. TSA Privacy contacted the individual and learned that he believed he had applied for a Known Shipper credential, confirmed that he had not actually submitted any application, and further learned that the individual had received incorrect guidance from airline staff regarding the need for a Known Shipper credential for a one-time shipment of electronics and did not qualify for a Known Shipper credential.

APPENDIX – PUBLISHED PRIVACY IMPACT ASSESSMENTS AND SYSTEM OF RECORDS NOTICES

Privacy Impact Assessments Published October 1, 2020 – March 31, 2021	
DHS Component and System Name	**Date Published**
DHS/ALL/PIA-046 Data Services Branch	1/5/2021
ALL/PIA-087 Law Enforcement Officers Safety Act Program	11/13/2020
ALL/PIA-088 Preventing Infectious Disease at DHS Facilities During Declared Public Health Emergencies	12/21/2020
ALL/PIA-089 International Biometric Interoperability Initiative	1/6/2021
CBP/PIA-006(i) Advance Passenger Information System	2/9/2021
CBP/PIA-065 WebEOC	10/29/2020
CBP/PIA-066 CBP Support of CDC for Public Health Contact Tracing	12/15/2020
CBP/PIA-066(a) CBP Support of CDC for Public Health Contact Tracing	2/8/2021
CBP/PIA-067 Unified Secondary	12/15/2020
CBP/PIA-068 CBP One Mobile Application	2/19/2021
CBP/PIA-069 CBP Translate Mobile Application	3/15/2021
CBP/PIA-064 Credibility Assessment and Polygraph Services	3/11/2021
CIS Ombudsman/PIA-001(a) Minor to CRMaaS-HP	2/18/2021
CISA/PIA-023 Infrastructure Protection (IP) Gateway	12/11/2020
CISA/PIA-036 Chemical Facility Anti-Terrorism Standards Program Suspicious Activity Reports	12/16/2020
CISA/PIA-037 CYBERSENTRY	1/25/2021
ICE/PIA-032(b) FALCON Search and Analysis System	1/21/2021
ICE/PIA-059 Information Technology Service Management - ServiceNow	1/12/2021
TSA/PIA-046(c) Travel Document Checker Automation Using Facial Recognition	1/27/2021
USCIS/PIA-084 ATLAS	10/30/2020
USCIS/PIA-085 Pangea	12/29/2020

System of Records Notices Published October 1, 2020 – March 31, 2021	
DHS Component and System Name	**Date Published**
ALL-023 Personnel Security Management	10/12/2020
ALL-046 Counterintelligence Program	12/13/2020
ALL-047 Declared Public Health Emergency	12/11/2020
CBP-018 Customs Trade Partnership Against Terrorism	3/22/2021
CBP-024 Intelligence Records System	12/12/2020

FEMA-014 Hazard Mitigation Planning and Flood Mapping Products and Services Records	1/10/2021
FEMA-015 Fraud Investigations and Inspections Division	3/22/2021
ICE-004 Bond Management Information System	10/13/2020
ICE-009 External Investigations	11/20/2020
ICE-018 Analytical Records	3/22/2021
USCG-061 Maritime Analytic Support System	11/23/2020
USSS-001 Criminal Investigation Information	10/13/2020
USSS-004 Protection Information System	10/13/2020