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

PRIVACY POLICY GUIDANCE MEMORANDUM

April 25, 2017

Memorandum Number: 2017-01

MEMORANDUM FOR: DISTRIBUTION LIST

FROM: Jonathan R. Cantor
Acting Chief Privacy Officer

SUBJECT: DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information

I. PURPOSE AND SCOPE

In 2007, the Department of Homeland Security (DHS) announced that it would treat all persons' personally identifiable information (PII),[1] regardless of citizenship, the same under the Privacy Act and extend its protections accordingly ("Mixed Systems policy").[2] President Trump issued Executive Order (E.O.) No. 13,768, *Enhancing Public Safety in the Interior of the United States* on January 25, 2017, which states that agencies may no longer extend the protections of the Privacy Act to those other than U.S. citizens and Lawful Permanent Residents (LPR). As such, DHS must change its 2007 policy. Instead, DHS will now treat all persons, regardless of immigration status, consistent with the Fair Information Practice Principles (FIPPs) and applicable law.[3] All DHS personnel must follow the legal and policy obligations outlined below.

---

[1] DHS defines PII as "any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, [lawful] permanent resident, visitor to the U.S., or employee or contractor to the Department." DHS Handbook for Safeguarding Sensitive Personally Identifiable Information/Privacy Policy Directive 140-10, *available at* www.dhs.gov/privacy.

[2] The Mixed System policy states "Mixed System" or "Mixed Systems" shall mean any System of Records that collects, maintains, or disseminates information, which is in an identifiable form, and which contains information about U.S. Persons and non-U.S. Persons. *See* DHS Privacy Policy Guidance Memorandum No. 2007-01/Privacy Policy Directive 262-12, *DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons, as amended, available at* www.dhs.gov/privacy.

[3] The FIPPs form the basis of the Department's privacy compliance policies and procedures governing the use of personally identifiable information (PII). These principles are: Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability and Auditing. *See* DHS Privacy Policy Guidance Memorandum No. 2008-01/Privacy Policy Directive 140-06, *The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security, available at* www.dhs.gov/privacy.

II. BACKGROUND

As a matter of law, the Privacy Act of 1974 (Privacy Act), as amended,[4] provides statutory privacy rights only to U.S. citizens and LPRs. In 2007, the DHS Privacy Office released Privacy Policy Guidance Memorandum 2007-01/Privacy Policy Directive 262-12, *DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons* ("Mixed Systems policy"). Under this policy, DHS extended Privacy Act protections to PII that was collected, used, maintained, or disseminated, and was to be retrieved by a personal identifier, in connection with a mixed system as a System of Records subject to the Privacy Act regardless of whether the information pertained to a U.S. citizen, LPR, immigrant, or non-immigrant. DHS extended these protections because of inherent difficulties in determining a person's current immigration status, which may change over time through naturalization or adjustment. Out of operational necessity and administrative efficiency, DHS continues to have systems that maintain information on both U.S. citizens and LPRs, as well as immigrants and non-immigrants to meet its mission requirements.

Section 14 of E.O. No. 13,768 requires that "[a]gencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information." Privacy Policy Guidance Memorandum 2007-01/Privacy Policy Directive 262-12 is inconsistent with Section 14 of E.O. 13,768.

III. AUTHORITY

The Chief Privacy Officer (CPO) has primary responsibility under Section 222 of the Homeland Security Act of 2002, as amended,[5] for privacy policy at DHS. This responsibility includes assuring that the use of technologies sustains and does not erode privacy protections relating to the use, collection, or disclosure of personal information. The CPO requires DHS employees to comply with this updated policy to ensure suitable privacy protections are appropriately afforded to all persons, regardless of citizenship and immigration status, in compliance with E.O. 13,768, for PII collected, used, retained, or disseminated by DHS. Pursuant to this responsibility, the CPO requires that the FIPPs serve as the framework for privacy policy and implementation at DHS.

Further, the CPO may investigate or report to the Secretary the Department's programs and operations as the CPO deems necessary or desirable.[6] This includes investigation of or reports regarding compliance with all policies established by the CPO, including the FIPPs.

[4] 5 U.S.C. § 552a.
[5] Homeland Security Act of 2002, Pub. L. No. 107-296, § 222, 116 Stat. 2135, 2155 (2002) (amended 2013).
[6] 6 U.S.C. § 142(b)(1)(B).

IV. PRIVACY POLICY

A. Fair Information Practice Principles (FIPPs)[7]

The CPO determined that the FIPPs serve as the foundational principles for privacy policy and implementation at DHS, regardless of immigration status. The FIPPs are a widely recognized framework for privacy law and policy used in many parts of the world.[8] The FIPPs help serve as a useful framework for the Department to analyze how to handle PII, comply with its continuing responsibilities under the numerous legal obligations that apply, as well as adhere to its commitments to its partners. The Department uses the eight FIPPs below to assess and enhance privacy protections by analyzing the nature and purpose of the collection and use of PII to fulfill DHS's mission. Nothing in E.O. 13,678 changes this responsibility.

i. Transparency

The Department must provide transparency for how it handles PII through various mechanisms, including Privacy Impact Assessments (PIA),[9] System of Records Notices (SORN),[10] Privacy Act Statements,[11] Privacy Compliance Reviews (PCR),[12] general notices, reports, investigations,[13] public meetings,[14] and the Freedom of Information Act (FOIA).[15] The DHS Privacy Office determines for the Department how to provide appropriate transparency for information collected, used, maintained, or disseminated. Even when not required by the Privacy Act or other legal obligations, DHS endeavors to include privacy notices on all information collections. The DHS Privacy Office is developing a template to guide Components when drafting privacy notices or privacy statements for information collections and will determine when such notice is required.

---

[7] The FIPPs first originated in the following report: Dep't of Health, Education, and Welfare (HEW), *Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems* (1973), *available at* https://www.justice.gov/opcl/docs/rec-com-rights.pdf.

[8] The background and history of the FIPPs as a privacy policy framework is discussed in depth in Privacy Policy Guidance Memorandum No. 2008-01/Privacy Policy Directive 140-06, *The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security*, *available at* www.dhs.gov/privacy. Nothing in this memorandum supersedes or replaces information and guidance that is provided by Privacy Policy Guidance Memorandum No. 2008-01. DHS uses the FIPPs in Privacy Impact Assessments, oversight activities, information sharing agreements, privacy policies, redress activities, and its other privacy responsibilities. The FIPPs have been expressly adopted by the Office of Management and Budget (OMB) and made applicable to the Federal Government in (1) OMB Circular No. A-130, *Managing Information as a Strategic Resource*, Appendix II, *Responsibilities for Managing Personally Identifiable Information*, 81 Fed. Reg. 49,689 (July 28, 2016); and (2) the National Institutes for Standards and Technology (NIST) Risk Management Framework, specifically described in NIST Special Publication (SP) 800-53 Rev. 4, App. J, *available at* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

[9] 6 U.S.C. § 142(a)(4); 44 U.S.C. § 3501 note.

[10] 5 U.S.C. § 552a(e)(4).

[11] 5 U.S.C. § 552a(e)(3).

[12] 6 U.S.C. § 142. *See also* https://www.dhs.gov/investigations-reviews. The CPO and the DHS Privacy Office conducts PCRs pursuant to its responsibility under Section 222 of the Homeland Security Act to assure that technologies sustain and do not erode privacy protections, and that the FIPPs are followed in handling PII.

[13] 6 U.S.C. § 142(b)(1)(B). *See also* https://www.dhs.gov/investigations-reviews.

[14] *See, e.g.*, the DHS Data Privacy and Integrity Advisory Committee (DPIAC), *available at* https://www.dhs.gov/privacy-advisory-committee.

[15] 5 U.S.C. § 552.

ii. Individual Participation

The Department should involve the person in the process of using PII and, to the extent practicable, seek the person's consent for the collection, use, dissemination, or maintenance of PII. People seeking access to any record held by DHS containing personal information or seeking to contest the accuracy of its content, may submit a FOIA request or Privacy Act request, as permitted by law, to DHS. Given the nature of some of the information in DHS systems (e.g., sensitive law enforcement or intelligence information), DHS may not always permit the person to gain access to or amend his or her record. Requests processed under the Privacy Act are also processed under FOIA; requesters covered by both statutes are always given the benefit of the statute with the more liberal release requirements. People not covered by the Privacy Act or Judicial Redress Act (JRA)[16] still may obtain access to records consistent with FOIA unless disclosure is prohibited by law or if the agency reasonably foresees that disclosure would harm an interest protected by an exemption.[17]

Components should also take note of other statutory, regulatory, or other information sharing agreements that provide access and amendment of Department records. For example, DHS has established the Traveler Redress Inquiry Program (DHS TRIP) to address perceived watchlist-related and other traveler screening redress inquiries. Additional processes exist that permit updating and correcting records held by the Department, consistent with other authorities.[18] Information sharing and systems that often aggregate data from multiple sources and increasingly look to newer tools such as data analytics should take advantage of opportunities to counter possible errors. These activities are consistent with the principle of individual participation; allowing people to update and amend records can reduce unnecessary errors, improve effectiveness and outcomes, and prevent waste at partner agencies that often rely on the same information.

iii. Purpose Specification

Purpose specification is linked to the Department's authorities to take action; in the absence of legal authority to act on the information, the Department should not collect the information. The Department must articulate the authorities that permit the collection of information about all persons maintained in DHS systems. The Department must also clearly state the purposes for which the information is intended to be used in applicable SORNs, PIAs, and notices. Planned uses must be compatible with the purpose for which DHS originally collected the information; the PIA must identify and explain this compatibility.

iv. Data Minimization

The Department collects only information that is relevant and necessary to accomplish the purposes specified in its notices and retains such information for only as long as is necessary to fulfill the purposes specified in its notices. Other laws, such as the Federal Records Act,[19] require agencies to determine schedules for record retention that are justified based on the purpose for which the

[16] *See* Appendix A, Judicial Redress Act of 2015.
[17] 5 U.S.C. § 552 (2016), *amended* by FOIA Improvement Act of 2016, Pub. L. No. 114-185, 130 Stat. 538 (June 30, 2016).
[18] *See, e.g.*, the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. §§ 1681-1681x, which also provides persons with the ability to amend records.
[19] *See* Federal Records Act of 1950, Pub. L. No. 81-754, 64 Stat. 585 (codified as amended in Chapters 21, 29, 31, and 33 of 44 U.S.C.).

information is collected and used.[20] The FRA process seeks to minimize the collection of information. DHS also places a special emphasis on reducing the use of sensitive PII, when practicable and possible, including Social Security numbers (SSN) and Alien Registration Numbers (A-Numbers).[21] DHS does not collect, use, maintain, and disseminate SSNs unless required by statute or regulation, or when pursuant to a specific authorized purpose.[22]

While Section 14 of E.O. 13,768 requires that "[a]gencies … ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information"; it does not require the collection of additional data specifically targeted at determining citizenship status when not otherwise required. Collecting additional data or building new systems interfaces to capture this information creates its own risks; reconfiguring systems in this manner would divert needed, limited resources from other priorities and could create cybersecurity risks. All of these factors must be considered when determining what data to include in a system. Through the Privacy Threshold Analysis (PTA) process, the DHS Privacy Office and the Component Privacy Officer help the Department determine the appropriate approach to ensure that only the needed data elements are collected.

v. Use Limitation

The Department uses information for the purposes specified in its SORNs, PIAs, and notices, and any sharing of such information outside the agency must be compatible with the purposes for which the information was originally collected. With respect to records covered under the Privacy Act or JRA, the Department may only use and share records with the written consent of the individual, unless one of twelve exceptions applies.[23] Consent for use and onward sharing must also be described in PIAs when required pursuant to the CPO's authority under the Homeland Security Act or under section 208 of the E-Government Act of 2002, which may apply to people other than U.S. citizens and LPRs.[24] Thus, seeking consent is always a preferable privacy practice, and consent should be sought when practical. The Privacy Act also requires that DHS describe how it uses and shares information external to the Department, known as "routine uses" in its SORNs, and ensure that such uses are compatible with the purpose for why the Department collected the records.[25] As a part of the DHS PIA process and privacy notice process, the Department must articulate the purpose and authorities for the collection of information as well as identify the categories of internal and external entities with whom it shares PII.

There is a risk of violating the Privacy Act when sharing or disclosing records if the immigration status of the subject is uncertain or simply not included in the individual record. Further, once a person changes status to a U.S. citizen or LPR, all records pertaining to that individual maintained in

[20] 44 U.S.C. § 3303.
[21] DHS Handbook for Safeguarding Sensitive Personally Identifiable Information/Privacy Policy Directive 140-10, *available at* www.dhs.gov/privacy.
[22] DHS Privacy Policy Guidance Memorandum No. 2007-02/Privacy Policy Directive 140-11, *Use of Social Security Numbers at the Department of Homeland Security, available at* www.dhs.gov/privacy.
[23] 5 U.S.C. § 552a(b).
[24] *See* 44 U.S.C § 3501 note; OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (Sept. 26, 2003).
[25] 5 U.S.C. § 552a(a)(7), (e)(4)(D). *See* Britt v. Naval Investigative Service, 886 F.2d 544 (3d Cir. 1987) (defining "compatibility" to require a "more concrete relationship or similarity, some meaningful degree of convergence, between the disclosing agency's purpose in gathering the information and in its disclosure" than simple relevance.)

DHS records systems are subject to the Privacy Act. This includes all records maintained by the Department on that individual prior to him or her becoming a U.S. citizen or LPR. Thus, when developing and negotiating information sharing and access agreements—particularly those that share data in bulk—the Department should take appropriate steps to account for the fact that a person's status, and therefore whether he or she is protected by the Privacy Act, may change during the life of the agreement.[26]

Absent a statutory requirement to disclose specific information, sharing decisions should be made with care. The DHS Privacy Office and component Privacy Officers work very closely with senior leadership and program managers not only to ensure that appropriate data are collected, but also to ensure that appropriate sharing, even on records not covered by the Privacy Act or JRA, may take place consistent with or when required by law to help accomplish mission objectives. All information sharing that relates to immigrants and non-immigrants must be described and justified in the appropriate PIA based on the FIPPs. There are other authorities in addition to the Privacy Act and JRA that can operate to limit how information is shared, depending on what the records are and with what entity the Department would like to share the records.[27] DHS employees should continue to exercise due diligence, and review the appropriate PIA or SORN for guidance with respect to sharing PII.[28] When in doubt, seek advice from appropriate component counsel, component privacy and FOIA officials, or the DHS Privacy Office.

vi. Data Quality and Integrity

The Department should rely on information only when it is reasonably considered accurate, relevant, timely, and complete. Failure to maintain accurate records serves to undermine efficient decision making, and can create the risk of errors. While the Privacy Act itself requires DHS to maintain accurate records, the Department should strive to maintain accurate records to the extent doing so would not otherwise interfere with ongoing enforcement investigation operations or intelligence activities. Further, PIAs are published, in part, to ensure that projects, programs, and systems maintain accurate data. In addition, collecting, maintaining, using, and disseminating accurate information helps the Department to efficiently meet its operational goals, prevent waste, and improve outcomes.

vii. Security

The Department protects all PII from inappropriate, unauthorized, or unlawful access, use, disclosure, or destruction. DHS complies with the Federal Information Security Modernization Act of 2014 (FISMA),[29] and has implemented an information security program to ensure appropriate safeguards are in place. Additional information security requirements may be defined in information sharing access agreements, interconnection security agreements, and the provisions of service contracts that contain specific security requirements. DHS SORNs and PIAs contain specific sections to address the manner in which information is securely maintained and protected. FISMA protects all sensitive information, including PII, regardless of the citizenship status of the person.

[26] *See* DHS Directive No. 262-05, *Information Sharing and Safeguarding* (Sept. 4, 2014); DHS Instruction No. 262-05-001, *DHS Information Sharing Environment* (Sept. 12, 2014).
[27] *See*, *e.g.*, Appendix A.
[28] All PIAs and SORNs are available at www.dhs.gov/privacy.
[29] Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014) (primarily codified at 44 U.S.C. chapter 35, subchapter II).

viii. Accountability and Auditing

The Department must be accountable for the use of information collected, maintained, and used in its systems. The Department demonstrates this accountability through a variety of mechanisms including those listed below:

- DHS provides transparency through various notice mechanisms including SORNs, PIAs, Privacy Act Statements, public meetings, and general notices.
- DHS conducts PCRs and Component Privacy Officers conduct privacy reviews of programs and operations.
- DHS provides training to all employees and contractors who have access to or use PII. DHS provides specific role-based training on systems that manage PII.
- DHS provides supplemental guidance including handbooks for handling and Safeguarding Sensitive Personally Identifiable Information at DHS[30] and the Privacy Incident Handling Guidance (PIHG).[31]
- DHS takes appropriate action, which can include investigations, when violations of its privacy policies are found.

B. Privacy Impact Assessments

The Department conducts PIAs to help implement privacy protections into new and existing programs, and to help develop strategies for mitigating identified privacy risks. As Privacy Policy Guidance Memorandum No. 2008-02/Privacy Policy Directive 140-09, *DHS Policy Regarding Privacy Impact Assessments* notes, senior leadership and program managers have the overall responsibility and commitment to ensure that DHS programs and initiatives protect privacy. The PIA process helps identify the privacy issues and risks and evaluate whether the programs and initiatives have adequately addressed these issues and risks. When conducting PIAs, Component Privacy Officers must address how the Department proposes to mitigate privacy risks that may arise with respect to different populations.[32] Any planned routine disclosures and sharing must be discussed in the PIA. In addition, as directed by the CPO, program managers must conduct PIAs on privacy-sensitive programs, initiatives, activities, or technologies that are not otherwise covered by the Privacy Act or E-Government Act.[33]

C. Privacy Compliance Reviews

The DHS Privacy Office and Component Privacy Officers conduct PCRs, which are designed to provide a constructive mechanism to improve a DHS program's ability to comply with assurances made in existing privacy compliance documentation and DHS Privacy Policies.[34]

---

[30] *See* DHS Handbook for Safeguarding Sensitive Personally Identifiable Information/Privacy Policy Directive 140-10, *available at* www.dhs.gov/privacy.
[31] *See* DHS Privacy Incident Handling Guidance (PIHG)/Privacy Policy Directive 140-07, *available at* www.dhs.gov/privacy.
[32] See DHS Privacy Policy Instruction No. 047-01-005, Component Privacy Officer (Feb. 2, 2017), *available at* www.dhs.gov/privacy.
[33] 6 U.S.C. § 142(a)(1),(4). *See also* Privacy Policy Guidance Memorandum No. 2008-02/Privacy Policy Directive 140-09, *DHS Policy Regarding Privacy Impact Assessments*, *available at* www.dhs.gov/privacy.
[34] The DHS Chief Privacy Officer conducts PCRs pursuant to 6 U.S.C. § 142(b). Component Privacy Officers conduct PCRs pursuant to DHS Privacy Policy Instruction No. 047-01-004, *Chief Privacy Officer Privacy Compliance Reviews* (Jan. 19, 2017), *available at* www.dhs.gov/privacy.

All Component Privacy Officers must create a review mechanism for their programs, similar to the DHS PCR process. Within one year of a request by the CPO, all Component Privacy Officers must conduct a Component privacy review of any programs identified by the CPO and report its findings and recommendations to the CPO. These reviews are designed to be public-facing to the extent they do not contain classified, law enforcement sensitive, or other sensitive information. Thereafter, Component Privacy Officers must conduct a privacy review or compliance evaluation on identified relevant programs and initiatives with outstanding recommendations, and coordinate activities and findings with the DHS Privacy Office.

D. Third Party Disclosure

When responding to an inquiry from a third party (i.e., a party who is not the subject of the record(s), a representative of the subject, or a party who is not covered under Official Sharing below) involving the disclosure of PII, all DHS personnel must perform an analysis under applicable law that ensures that the information being shared is appropriate for release to the public.[35] Such an analysis seeks to balance the public's right to know about the functions and operations of the Government—in other words how DHS enforced the law or complied with a legal obligation—as compared to the interest of the subject of the request in keeping his or her identity and activities private. Depending upon the nature of the encounter between DHS and the subject, the notoriety of the subject's actions may diminish the extent to which those actions may remain private.[36] Third party disclosures include responses to individual members of the public, members of the U.S. Congress who are not Committee chairs acting on behalf of the Committee,[37] and the media. Questions concerning the analysis should be referred to Component Privacy Officers and FOIA Officers.

Discretionary disclosure of confirmed non-U.S. citizen and non-LPR PII is permitted when no other restrictions or prohibitions on the disclosure apply, subject to review under the balancing analysis described above. Components must develop specific processes to manage these disclosures and submit these procedures to the DHS Privacy Office for approval prior to implementation.

E. Official Sharing

Official Sharing means disclosures that take place pursuant to requests from Congressional Committee Chairpersons acting on behalf of their committees, federal courts, federal, state, local, tribal, and foreign law enforcement and other administrative agencies having a need for information from DHS files for the performance of their official duties. For U.S. citizens, LPRs, and those covered by the JRA, these disclosures are generally made pursuant to routine uses that are listed in SORNs or pursuant to another authorized disclosure stated in the Privacy Act.[38] All official sharing requests that apply to U.S. citizens, LPRs, and those covered by the JRA must still be analyzed to determine whether a routine use or other exception to the Privacy Act disclosure provisions applies.

With respect to persons who are not covered by the Privacy Act or JRA, employees must use a FIPPs analysis when reviewing official sharing requests. This analysis requires a determination that the use of the records proposed is consistent with the purpose for which DHS collected the records. Any routine or regular sharing must be described in the applicable PIA and privacy notice. Although

[35] *See* Appendix A.
[36] *See* 5 U.S.C. §§ 552(b)(6), (b)(7)(C).
[37] *See* 5 U.S.C § 552a(b)(9).
[38] 5 U.S.C. § 552a(b).

E.O. 13,768 excludes information relating to persons not covered by the Privacy Act from being subject to the Privacy Act, the authorized disclosure exceptions, including routine uses listed in the applicable SORNs of the Privacy Act, may continue to be good guidance as to whether a disclosure is consistent with the purpose for the collection of the information, and generally the FIPPs framework.

With respect to information sharing activities, Department employees must confirm whether an agreement (e.g., information sharing access agreement, memorandum of understanding, memorandum of agreement), federal statute, or other legal authority permits the sharing and follows the terms of any applicable agreement or arrangement. Also, notwithstanding specific authority permitting the sharing of information, there may exist other policy considerations that would affect DHS's decisions whether to share information. Finally, the Department requires protections on further dissemination of the records beyond the requestor's agency or organization, and coordination with the DHS Office or Component responsible for acquiring the records subject to being shared to avoid operational conflicts.

F. Breaches of Personally Identifiable Information

The Department has a duty to safeguard PII in its possession, and to prevent the compromise of PII in order to maintain the public's trust in DHS. The Department has established policy and procedures for DHS personnel to follow upon the detection or discovery of a suspected or confirmed cybersecurity or non-cybersecurity incident involving the loss of PII (regardless of citizenship or immigration status of the subject[s]). The Department's Privacy Incident Handling Guidance (PIHG) serves this purpose by informing DHS and its components, employees, senior officials, and contractors of their obligation to protect PII, and by establishing procedures defining how they must respond to a breach of PII.[39] The PIHG also imposes individual accountability for compliance. Finally, OMB sets forth federal agency policy[40] on incidents and breaches of PII in accordance with FISMA. This policy is applicable to all individuals' information, regardless of citizenship or immigration status.

G. Component-Level Implementing Guidance

Component Privacy and FOIA Officers, in coordination with appropriate personnel, must create component-level guidance documents—consistent with this policy—to address their unique uses of PII. All component-level guidance documents must be approved by the DHS Privacy Office.

V. CANCELLATION

Privacy Policy Guidance Memorandum 2007-01/Privacy Policy Directive 262-12, *DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons* is hereby cancelled.

---

[39] *See* DHS Privacy Incident Handling Guidance (PIHG)/Privacy Policy Directive 140-07, *available at* www.dhs.gov/privacy.

[40] OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (Jan. 3, 2017). PII is defined in M-17-12 as it is in OMB Circular A-130. Further, incidents and breaches are defined in M-17-12.

Appendix A

Applicable Laws and Other Authorities

There are Constitutional, statutory, and regulatory authorities that may grant people rights of privacy or restrict disclosure of PII that continue to bind DHS. These authorities may apply regardless of the subject's immigration status. These authorities described in Appendix A do not constitute an exhaustive list. DHS must use due diligence to determine whether people have privacy rights under authorities not listed in Appendix A.

1. U.S. Constitution

A right to privacy has been found in a number of Amendments to the United States Constitution. For example, people have a right to the privacy of their associations and beliefs under the First Amendment.[41] In addition, people have a reasonable expectation of privacy in their homes and personal effects.[42] Additionally, privacy rights have been found to exist as a matter of liberty and due process in both the Fifth and Fourteenth Amendments.[43] The right to privacy has also been found to exist in the Ninth Amendment.[44] With some exceptions, constitutional rights apply to all people in the United States and to U.S. citizens wherever they may be.[45]

2. Privacy Act

The Privacy Act provides a number of statutory privacy rights to individuals, which it defines as U.S. citizens and LPRs.[46] Individuals have the right to access and amend their records contained in a DHS system of records, unless properly exempted from one or more provisions of the Privacy Act because of national security, criminal, investigatory, civil, and administrative enforcement requirements. DHS may not disclose an individual's records in a system of records without consent unless permitted by an authorized disclosure exception.[47] The Privacy Act also provides notice to individuals about the existence of the system and the Department's authority for collecting, maintaining, using, and disseminating PII through the use of Privacy Act notices, published SORNs, and published Privacy Act rulemakings.

The Department has established procedures and published rules implementing the Privacy Act on how, for instance, individuals can request access and amendment of their records, and requirements placed upon the Department with regard to data security and integrity and information management.[48] The Department is obligated to ensure that records are accurate, relevant, timely, and complete as is reasonably necessary to assure fairness to the individual as part of a Department

[41] *See* National Ass'n for Advancement of Colored People v. State of Ala. ex rel. Patterson, 357 U.S. 449 (1958). "This Court has recognized the vital relationship between freedom to associate and privacy in one's associations. […] Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs." Cf. United States v. Rumely, 345 U.S. 41, 56-58 (1953) (concurring opinion).
[42] Katz v. U.S., 389 U.S. 347 (1967) (Harlan, J. concurring); Kyllo v. U.S., 533 U.S. 27 (2001).
[43] Griswold v. Connecticut, 381 U.S. 479 (1965); Lawrence v. Texas, 539 U.S. 558 (2003).
[44] Griswold v. Connecticut, 381 U.S. 479 (1965) (Goldberg, J. concurring).
[45] U.S. v. Curtiss-Wright Export Corp., 299 U.S. 304 (1936)
[46] 5 U.S.C. § 552a(a)(2).
[47] 5 U.S.C. § 552a(b).
[48] 6 C.F.R. §§ 5.20-5.36. *See generally* 5 U.S.C. § 552a(e).

determination.[49] DHS must maintain only information that is relevant and necessary to accomplish its statutory mission under law.[50] Individuals may seek judicial redress for Privacy Act violations, including wrongful disclosure.[51] Certain exemptions to these requirements exist and may be claimed in the case of national security, law enforcement, or other bases.[52]

Once a person changes status to a U.S. citizen or LPR, all records on that individual maintained by DHS are subject to the Privacy Act. This includes all records maintained by the Department on that individual prior to the individual becoming a U.S. citizen or LPR. Employees and contractors may be charged criminally for certain willful violations of the Privacy Act.[53]

3. Judicial Redress Act of 2015

The Judicial Redress Act of 2015, Pub. L. 114-126 (JRA) (February 24, 2016), codified at 5 U.S.C. § 552a note, extends provisions of the Privacy Act to non-U.S. citizens and non-LPRs who are citizens of countries that have been designated pursuant to procedures identified within the JRA.[54] The JRA applies only to information shared with the U.S. Government by a public or private entity from a designated country for purposes of preventing, investigating, detecting, or prosecuting criminal offenses, known as "covered records" under the JRA. Information collected from other sources or for other purposes is not covered. Further, the JRA provides the civil remedies of the Privacy Act to citizens of such designated covered countries for wrongful disclosure of their records by designated federal agencies, including DHS. Individuals covered by the JRA have been granted the same administrative rights for access and amendment for records at those designated federal agencies; and may bring suit in the U.S. district courts for denying access or amendment, or for wrongfully disclosing information contained in a Privacy Act protected system of records. The exemptions contained in the Privacy Act itself limiting access, amendment, and judicial redress in certain situations continue to apply to citizens of designated countries.

4. Freedom of Information Act

The Freedom of Information Act (FOIA), 5 U.S.C. § 552, provides that any person regardless of citizenship or immigration status has a right to obtain records, including by seeking access to records held about oneself, maintained by a federal agency, subject to nine exemptions.[55] DHS processes all requests for records using a FOIA analysis, as opposed to other official sharing channels (e.g., law

[49] 5 U.S.C. § 552a(e)(5).
[50] 5 U.S.C. § 552a(e)(1).
[51] 5 U.S.C. § 552a(g).
[52] 5 U.S.C. § 552a(j) & (k).
[53] 5 U.S.C. § 552a(i).
[54] The JRA implements the judicial redress provisions of the *Agreement between the United States of America and the European Union on the Protection of Personal Information Relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offenses*, June 2, 2016, known as the Data Protection and Privacy Agreement (DPPA) or "Umbrella Agreement." This agreement, like the JRA, also constitutes applicable law for purposes of Executive Order 13,768. As of the date of this memorandum, the European Union and most of its Member States (the Department of Justice has not received notice from the United Kingdom and Denmark to date and is not designated) have been designated by the Attorney General as "covered countries," and DHS has been designated in its entirety as a designated agency pursuant to the JRA. *See* Judicial Redress Act of 2015; Attorney General Designations, 82 Fed. Reg. 7860 (Jan. 23, 2017).
[55] *See generally* 5 U.S.C. § 552. Exemptions 6 and 7(C) limit personal information from disclosure to third party requesters. 5 U.S.C. §§ 552(b)(6), (b)(7)(C).

enforcement and investigations[56], intelligence).[57] This analysis does not change as a result of cancellation of the Mixed Systems policy.

Prior to releasing a person's PII pursuant to a FOIA request from a third party, or when DHS proactively discloses records to a member of the general public and the person has not expressly consented to or approved of the disclosure,[58] the personal privacy interests of the subject, regardless of immigration status, must be balanced against the public interest in the requested information.[59] The Supreme Court has determined that the privacy interest inherent in exemptions 6 and 7(C) belongs to the person and not the agency.[60] The only public interest to be considered is whether the requested information would shed light on the agency's performance of its statutory duties. Information that does not reveal the operations and activities of the Government does not satisfy the public interest requirement.[61]

5. The E-Government Act of 2002

Section 208 of the E-Government Act of 2002[62] provides privacy protections for all PII held electronically by the U.S. Government, regardless of whether it pertains to a U.S. citizen, LPR, immigrant, or non-immigrant. Section 208 requires that all Executive Branch agencies, such as DHS, address privacy risks when agencies develop or procure new or modified technologies to collect,

---

[56] For example, when information is being disclosed proactively to a witness, who is a member of the public, in furtherance of an investigation, there is no need for a FOIA analysis.

[57] A FOIA request is a written request to a federal agency for access to records. When the subject of the records is the requestor, this is a "first party" request. When the subject of the requested records is another person, organization, or a topic of interest, and the requestor is a member of the public, media, or a member of Congress acting on behalf of another or in his or her individual capacity, this is a "third party" request. Moreover, requesters covered by the Privacy Act or JRA who seek records concerning themselves are afforded the benefit of the access provisions of both FOIA and the Privacy Act and obtain the benefit of whichever statute affords the most access. The term "FOIA request" also includes any such "first party" requests when an agency determines that it must search beyond its Privacy Act systems of records or when the agency applies a Privacy Act exemption and therefore looks to FOIA to afford the greatest possible access. Entities within the Federal Government, such as other agencies, courts, and Congress and its committees, do not file FOIA requests. *See* 5 U.S.C. § 551(2) (defining person for purposes of the Administrative Procedure Act (APA), which is incorporated into the FOIA). Requests for records from individual members of Congress, however, acting on behalf of themselves and not in their capacity as a Committee Chair, are reviewed and analyzed pursuant to the FOIA. *See* Dep't of Justice FOIA Update, Vol. V, No. 1, at 3-4 (distinguishing between individual members of Congress and Congress as an institutional entity, which exercises its authority through its committee chairs).

[58] Because the privacy interests protected by FOIA belong to the person, courts have held that people can sue to prevent agencies from disclosing records pursuant to a request under the APA, 5 U.S.C. §§ 701-706 (2006). *See* Campaign for Family Farms v. Glickman, 200 F.3d 1180, 1187-89 (8th Cir. 2000) (deciding that judicial review based on administrative record according to "arbitrary, capricious, or not in accordance with law" standard applies to so-called "reverse FOIA" cases protecting identities of those who signed petition, because release of the records would reveal position on referendum and "would vitiate petitioners' privacy interest in secret ballot").

[59] *See* U.S. Dep't of State v. Ray, 502 U.S. 164, 175-79 (applying the traditional analysis of privacy interests under FOIA to Haitian nationals).

[60] DOJ v. Reporters Comm. For Freedom of the Press, 489 U.S. 749, 763-65 (1989).

[61] *Id*.

[62] 44 U.S.C. § 3501 note. Section 202(i) of the E-Government Act exempts "national security systems", as defined by 40 U.S.C. § 11103(b), from certain provisions of the Act, including the publishing of PIAs. *See also* OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (Sept. 26, 2003). However, the CPO may require an office to draft and complete a PIA on a national security system. Although these PIAs are not made public because of national security concerns they serve as a key component of ensuring that classified programs have appropriately considered and implemented privacy protections. *See* Privacy Policy Guidance Memorandum No. 2008-02/Privacy Policy Directive 140-09, *DHS Policy Regarding Privacy Impact Assessments, available at* www.dhs.gov/privacy.

maintain, use, or disseminate PII by publicly posting a PIA.[63] Section 208 also requires the Department to develop privacy policies on all public-facing webpages that inform visitors to the website about information collection activities on those pages, including whether those collections are voluntary and how to consent to the uses of information provided.[64] These guidelines apply not only to the webpage itself, but also to the use of all web measurement and customization technologies on the webpages[65] and to the Department's use of third-party websites and applications for these purposes, such as social media.[66]

6. The Paperwork Reduction Act

Before requiring or requesting information from the public, the Paperwork Reduction Act (PRA)[67] requires federal departments and agencies to seek public review and comment before submitting forms and information collections for review and approval by the Office of Management and Budget (OMB). As part of the PRA package, the Department must submit applicable privacy compliance documentation. In 44 U.S.C. § 3502(3) and 5 C.F.R. 1320.3(c), the PRA applies to collections of information from the public using identical questions posed to, or reporting or recordkeeping requirements imposed on, ten or more persons, regardless of citizenship. The requirements of the PRA apply to voluntary collections as well as mandatory collections. These procedures help limit the amount of information agencies collect.

7. Federal Records Act

The Federal Records Act of 1950 (FRA)[68] requires that "the head of each Federal agency shall make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency and designed to furnish the information necessary to protect the legal and financial rights of the Government and of persons directly affected by the agency's activities."[69]

The Federal Records Act provides historical support for several FIPPs, including individual participation by ensuring the appropriate maintenance of a record that allows access rights to the subject of the record and data minimization by limiting the collection of PII and ensuring the destruction of PII when there is no longer a business, legal, or historical need for the record.

[63] For more information on PIAs, *see* Privacy Policy Guidance Memorandum No. 2008-02/Privacy Policy Directive 140-09, *DHS Policy Regarding Privacy Impact Assessments, available at* www.dhs.gov/privacy.
[64] *See* 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); OMB Memorandum M-17-06, *Policies for Federal Agency Public Websites and Digital Services* (Nov. 8, 2016).
[65] *See* OMB Memorandum M-10-22, *Guidance for Online Use of Web Measurement and Customization Technologies* (June 25, 2010).
[66] *See* OMB Memorandum M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications* (June 25, 2010)
[67] 44 U.S.C. §§ 3501-3521.
[68] Federal Records Act of 1950, Pub. L. No. 81-754, 64 Stat. 585 (codified as amended in Chapters 21, 29, 31, and 33 of 44 U.S.C.).
[69] 44 U.S.C. § 3101.

8. Homeland Security Act

Section 221 of the Homeland Security Act, 6 U.S.C. § 141, requires DHS to establish procedures to limit re-dissemination of information, ensure confidentiality and security of shared information, protect the constitutional and statutory rights of subjects of shared information, and provide data integrity through the timely removal and destruction of obsolete or erroneous information.

9. The Violence Against Women Act

The Violence Against Women Act (VAWA), 8 U.S.C. § 1367, generally prohibits DHS from disclosing any information regarding individuals who have applied for or received immigration benefits under the VAWA, T non-immigrant status, or U non-immigrant status, unless a statutory exception applies (e.g., for legitimate law enforcement or national security purposes). This prohibition against disclosure applies to any information about the individual, not simply the information maintained in the specific petition or application for the benefit.

10. Child Victims' and Child Witnesses' Rights

Section 225 of the Crime Control Act of 1990, 18 U.S.C. § 3509(d)(1), provides for the confidentiality of information about child witnesses. It does this by mandating: 1) that all documents containing the name or any other identifying information about a child be kept in a secure place; and 2) prohibiting the disclosure of any of those documents except in certain circumstances, such as disclosures to persons who, by reason of their participation in the proceedings have a reasons to know such information. These provisions can, in part, be complied with by filing documents under seal or requesting a protective order under subsections 3509(d)(2) and (3). In addition, these mandates are applicable to all law enforcement, government employees or their agents as well as court personnel, the defendant, defendant's employees and members of the jury.

11. Use of Juvenile Records

Section 508 of the Juvenile Justice and Delinquency Prevention Act of 1974, 18 U.S.C. § 5038 protects the disclosure of information related to federal juvenile delinquency records. Federal agencies may not release information about federal juvenile delinquency records, except in limited circumstances. The statute requires agencies to respond to any inquiry about juvenile records in the same manner as responses made about persons who have never been involved in delinquency proceedings. The prohibitions on disclosure of federal delinquency records do not apply to state juvenile delinquency records.

12. Immigration and Nationality Act

Section 264 of the Immigration and Nationality Act, 8 U.S.C. § 1304(b), protects from disclosure registration and fingerprint records collected under 8 U.S.C. §§ 1301 and 1302. The statute allows for an exception to provide fingerprints and photographs to federal, state, and local law enforcement agencies, upon request. Federal law also restricts the disclosure of information relating to persons who have Temporary Protected Status (TPS),[70] 8 U.S.C. § 1254a(c)(6), or Legalization claims, 8 U.S.C. § 1255a(c)(4), including Seasonal Agricultural Worker (SAW) claims, 8 U.S.C. § 1160(b)(5)

[70] 8 C.F.R. § 244.16 is the implementing regulation for TPS confidentiality.

and (6). Likewise, visa information is protected by Section 222(f) of the Immigration and Nationality Act, 8 U.S.C. § 1202(f).

13. Cybersecurity Information Sharing Act (CISA)

CISA[71] creates a voluntary cybersecurity information sharing process that encourages public and private entities to share cyber threat information while protecting classified information, intelligence sources and methods, and privacy and civil liberties. On June 15, 2016, DHS and the Department of Justice (DOJ) jointly issued Privacy and Civil Liberties Final Guidelines, which are based on the FIPPs.[72]

14. International Arrangements, Agreements, and Mechanisms[73]

The United States is a party to numerous binding international agreements that similarly affect the manner in which DHS may disclose information.[74] The Department will continue to comply with the provisions contained in such legally binding agreements, including privacy protections such as access, rectification, or judicial redress to records containing PII. In addition, DHS will continue to comply with any provisions that place restrictions on the use and further sharing by DHS of records covered under the agreement or other information sharing arrangements or mechanisms. Further, DHS components may develop their own protocols for discretionary sharing of PII for administrative, law enforcement, or intelligence purposes. Questions regarding the applicability and restrictions of any agreement or information sharing arrangement should be referred to the appropriate DHS counsel and privacy officer.

15. Regulatory Restrictions

Subject to certain exceptions, the asylum regulations at 8 C.F.R. § 208.6 generally prohibit the disclosure of information contained in or pertaining to asylum applications, any credible fear determinations conducted under 8 C.F.R. § 208.30, or any reasonable fear determinations conducted under 8 C.F.R. § 208.31. DHS has extended the application of the asylum confidentiality regulations to information contained in or pertaining to refugee applications. Executive Order No. 13,768 does not affect that policy.

In addition, DHS regulations protect information regarding pre and post order detainees, 8 C.F.R. § 236.6, and protect from disclosure information that is subject to an Immigration Judge's protective

[71] Cybersecurity Act of 2015, Pub. L. No. 114-113, Division N § 104(c), 129 Stat. 2242, 2942 (2015).
[72] https://www.us-cert.gov/sites/default/files/ais_files/Privacy_and_Civil_Liberties_Guidelines_(Sec%20105(b)).pdf.
[73] Reciprocity is a fundamental condition of international relations and one the U.S. Government has followed with the treatment of persons and exchanges of information. Indeed, it is a fundamental structure of many international agreements including arms control, trade and commerce, and law enforcement. Arthur Nussbaum, *A Concise History of the Law of Nations* (The Macmillion Co., New York, 1954); Robert O. Keohane, *Reciprocity in International Relations*, 40 INT'L ORG. 1 (1986). Even the Supreme Court has observed, "Public officials should bear in mind that 'international law is founded upon mutuality and reciprocity. . . .'" Breard v. Pruett, 134 F.3d 615, 622 (4th Cir.), cert. denied sub nom. Breard v. Greene, 118 S.Ct. 1352 (1998) quoting Hilton v. Guyot, 159 U.S. 113, 130 (1895).
[74] Applicable laws include international agreements. *See, e.g.*, Am. Ins. Ass'n v. Garamendi, 539 U.S. 396, 398 (2003) (international agreements preempt state law).These include the Data Protection and Privacy Agreement (DPPA), the Passenger Name Record (PNR) Agreement with the European Union, as well as numerous Mutual Legal Assistance Treaties (MLATs), Preventing and Combating Serious Crime (PCSC) Agreements, and Customs Mutual Assistance Agreements (CMAAs) with foreign governments.

order, 8 C.F.R. § 1003.46. Although not an exhaustive list, these regulations are an indicia of regulatory restrictions on disclosure applicable to all persons regardless of immigration status. These authorities are not changed by E.O. 13,768.