9110-9B-P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

6 CFR Part 5

[Docket No. DHS-2021-0020]

RIN 1601-AB04

Privacy Act of 1974

AGENCY: Office of the Secretary, Department of Homeland Security.

ACTION: Notice of proposed rulemaking.

SUMMARY: The Department of Homeland Security (DHS or Department) is proposing to amend its regulations under the Privacy Act of 1974. DHS is proposing to update and streamline the language of several provisions. DHS invites comment on all aspects of this proposal.

DATES: Comments must be received on or before **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: You may submit comments, identified by docket number DHS-2021-0020, by one of the following methods:

- Federal e-Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.
- Mail: Lynn Parker Dupree, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

Instructions: All submissions received must include the agency name and docket number for this notice. All comments received may be posted without change to http://www.regulations.gov, including any personal information provided.

Docket: For access to the docket to read background documents or comments received, go to http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: Lynn Parker Dupree, (202) 343-1717, Privacy@hq.dhs.gov, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

SUPPLEMENTARY INFORMATION:

I. Background:

The Secretary of Homeland Security has authority under 5 U.S.C. 301, 552, and 552a, and 6 U.S.C. 112(e) to issue Privacy Act regulations. That authority has been delegated to the Chief Privacy Officer of the Department. *See* DHS Del. No. 13001, Rev. 01 (June 2, 2020).

On January 27, 2003, DHS published an interim rule in the **Federal Register** (68 FR 4056) that established DHS procedures for obtaining agency records under the Privacy Act, 5 U.S.C. 552a. DHS has since issued minor procedural amendments to the interim rule, *see* 85 FR 11829 (Feb. 28, 2020), but DHS has not issued a more comprehensive update since 2003.

On November 22, 2016, DHS issued a final rule amending the Department's regulations under the Freedom of Information Act (FOIA), 6 CFR Part 5, Subpart A, in order to update and streamline the language of several procedural provisions, to incorporate changes brought by the amendments to the FOIA under the Open Government Act of 2007 and FOIA Improvement Act of 2016, and to reflect developments in the case law. *See* 81 FR 83625.

DHS now proposes to revise its Privacy Act regulations at 6 CFR Part 5, Subpart B, to conform with Subpart A, to clarify and streamline the language of several provisions, to incorporate the additional rights granted under the Privacy Act by way of the Judicial Redress Act of 2015 (JRA), and to reflect developments in the case law. Further, DHS proposes to revise Appendix A to Part 5 – *FOIA/Privacy Act Offices of the Department of Homeland Security* – to reflect updates to the proper offices in receiving FOIA and

Privacy Act requests. This appendix would also replace Appendix I to Subpart A. As such, DHS proposes to revise its FOIA regulations at 6 CFR Part 5, Subpart A, for the limited purpose of replacing references to Appendix I to Subpart A with references to Appendix A to Part 5.

DHS describes the primary proposed changes in the section-by-section analysis below. DHS invites public comment on each of the proposed changes described, as well as any other matters within the scope of the rulemaking.

II. Section by Section Analysis

The proposed rules continue to inform the public of the responsibilities of DHS in conjunction with requests received under the Privacy Act as well as the requirements for filing a proper Privacy Act or Judicial Redress Act request.

Section 5.20 General Provisions.

DHS is proposing to amend this section to be consistent with Subpart A and incorporate changes made to 5 U.S.C. 552a by way of the Judicial Redress Act of 2015 (JRA), Pub. L. No. 114-126 (Feb. 24, 2016).[1] Proposed section 5.20(a)(2) references the JRA, the term "covered persons," and any Federal Register notice making a JRA designation. Proposed section 5.20(a)(3) would remove the following language in existing section 5.20(a)(2): "Except to the extent a Department component has adopted separate guidance under the Privacy Act, the provisions of this subpart shall apply to each component of the Department. Departmental components may issue their own guidance under this subpart pursuant to approval by the Department." This proposal would remove a reference to separate guidance developed by Components. Components may continue to

[1] The Judicial Redress Act of 2015, 5 U.S.C. § 552a note, extends certain rights of judicial redress established under the Privacy Act of 1974, 5 U.S.C. § 552a, to citizens of certain foreign countries or regional economic organizations. Specifically, the Judicial Redress Act enables a "covered person" to bring suit in the same manner, to the same extent, and subject to the same limitations, including exemptions and exceptions, as an "individual" (i.e., a U.S. citizen or lawful permanent resident) may bring and obtain with respect to the: 1) intentional or willful unlawful disclosure of a covered record under 5 U.S.C. 552a(g)(1)(D); and 2) improper refusal to grant access to or amendment of a covered record under 5 U.S.C. 552a(g)(1)(A) & (B).

issue their own guidance under this subpart pursuant to approval by the Department; however, specific authorization for component guidance is not necessary to be included in the regulatory text.

DHS is proposing to amend the definition of "Component," to be consistent with the definition at 6 CFR 5.1(b). This definitional change will not result in a change in practice.

DHS is also proposing to add a definition of "individual," in paragraph (b)(6). This definition includes a U.S. citizen, a lawful permanent resident, and a "covered person" as defined under the JRA. The JRA extends the access and amendment provisions of the Privacy Act to covered persons for access and amendment requests of covered records, as defined by the JRA. As such, the term "individual" includes the term "covered persons," but only to the extent that this subpart applies to access and amendment requests for covered records, as defined below.

DHS is also proposing to add a definition of the term "records" to make clear DHS relies on the definition of "record" in the Privacy Act. *See* 5 U.S.C. 552a(a)(4). But in cases that fall under the JRA, the JRA's definition of "covered record" would apply. Under the JRA, the term "covered record" has the same meaning for a covered person as a record has for an individual under the Privacy Act, once the covered record is transferred (1) by a public authority of, or private entity within, a country or regional economic organization, or member country of such organization, which at the time the record is transferred is a covered country; and (2) to a designated Federal agency or component for purposes of preventing, investigating, detecting, or prosecuting criminal offenses. These changes are consistent with current DHS practice.

DHS also proposes to amend section 5.20(d) by replacing the term "exemption" with the term "exception," to be consistent with terminology within the Privacy Act.

Section 5.21 Requests for Access to Records.

DHS is proposing multiple changes to this section to be consistent with the similar provision in Subpart A regarding requirements for making FOIA requests. *See* 6 CFR 5.3. These conforming changes would be explanatory in nature and would not result in a departure from current practice.

Further, DHS proposes to amend paragraph (a) to specifically refer to JRA requests. Also, DHS proposes to add paragraph (b) to account for requests for Privacy Act records that are covered by a Government-wide SORN for which one Federal Agency writes the policy governing the subject records. In some cases, although DHS may have copies of such records, the Federal Agency that writes the policy for such records also has physical custody over the original records and retains authority over the records. As a general matter, a government-wide system of records is appropriate when one agency has government-wide responsibilities that involve administrative or personnel records maintained by other agencies. For example, the Office of Personnel Management has published a number of government-wide SORNs relating to the operation of the Federal Government's personnel programs. If records are sought that are covered by a Government-wide SORN and requested of DHS, DHS will consult or refer such request, only as applicable and necessary, to the corresponding agency having authority over such records for further processing. DHS will acknowledge to the requester that is referring the request to another agency or consulting with that agency when processing the request.

In addition, DHS is proposing to add additional language to current paragraph (b), now proposed paragraph (c), to address circumstances where the request does not adequately describe the records sought. This additional language comports with 6 CFR 5.3(c) for consistency with FOIA requests being made.

Further, DHS proposes changes to current paragraph (c), now proposed paragraph (d), regarding payment of fees to comport with procedures for payment for fees processed under the FOIA pursuant to 6 CFR 5.11.

Also, DHS proposes to amend paragraph (e), now proposed paragraph (f), to further clarify, consistent with 5 U.S.C. 552a(h), that a court of competent jurisdiction can determine an individual to be incompetent "due to physical or mental incapacity or age." Currently, the regulations only refer to a court's determination of incompetence but lacks this additional detail that is included in the statute.

Finally, DHS proposes to amend paragraph (f), now proposed paragraph (g), by adding a procedure by which a requester may submit proof that a third party is deceased (e.g., a copy of a death certificate or an obituary) and therefore no longer has any Privacy Act rights. Further, DHS is proposing to give each Component flexibility in requiring more information, if necessary, depending on the record, to verify that a third party has consented to disclosure.

Section 5.22 Responsibility for Responding to Requests for Access to Records.

DHS is proposing to amend this section to be consistent with Subpart A. Proposed paragraph 5.22(c) would now include a reference to the JRA, as well as including references to 6 CFR 5.4(d) and (e). DHS would eliminate existing paragraphs 5.22(e) and (f) as duplicative, but include in paragraph 5.22(c) some language originally provided for in existing paragraph 5.22(e).

Finally, pursuant to 5 U.S.C. 552a(f)(3), DHS proposes to amend existing paragraph (f), now paragraph (d), release of medical records, to provide more detail on when medical records may be released to the subject. In particular, DHS proposes to provide more detail on what special procedures DHS will follow when it receives an access request for medical records that include psychological records, and DHS determines that direct release of such records is likely to adversely affect the individual who is requesting access, such that direct release would be reasonably likely to cause harm or endanger physical life or safety of the subject individual or others. Further, it must be acknowledged that this provision applies to Privacy Act access requests. Some

components may rely on other additional regulations, and other implementing agency practices and policies derived from such regulations, which may establish separate, special procedures for such purposes. For instance, medical records held by covered entities within the U.S. Coast Guard (USCG) are subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The USCG follows the U.S. Department of Health and Human Services' implementing regulations at 44 CFR parts 160 and 164, as implemented in the Department of Defense's Manual 6025.18, including special rules for accessing protected health information related to substance abuse disorder programs. Finally, DHS proposes to eliminate the requirement that final review and decision on appeals of disapprovals of direct release will rest with the General Counsel, but rather to rely generally on subsection 5.25 for administrative appeals.

Section 5.23 Responses to Requests for Access to Records.

DHS is proposing to amend this section to be consistent with the similar provision in Subpart A with respect to responding to FOIA requests, including providing an acknowledgement letter and an assigned individualized tracking number if the request will take longer than 10 working days to process, since DHS processes Privacy Act requests under the FOIA as well, and responding within 20 working days from when a request is received to determine whether to grant or deny the request unless there are unusual or exceptional circumstances. *See* 6 CFR 5.6. Further, proposed paragraph 5.23(a) references the JRA. Finally, it was noted in this section that for purposes of responding to a JRA access request, a covered person is subject to the same limitations, including exemptions and exceptions, as an individual is subject to under section 552a of title 5, United States Code, when pursuing access to records.

Section 5.24 Classified Information.

DHS is proposing to amend this section to consolidate current paragraph 5.22(e) and this section. The resulting text would be consistent with the similar provision at 6 CFR 5.4(e).

Section 5.25 Administrative Appeals for Access Requests.

DHS is proposing to amend the title of this section to be more specific regarding the types of appeals processed by DHS under this section, because administrative appeals on amendment requests are governed by section 5.26(c). Also, DHS is proposing to amend this section to be consistent with the similar provision in Subpart A on access appeals, including providing that DHS will make a decision on an appeal in writing generally twenty (20) working days after receipt unless the time limit for responding to an appeal may be extended provided the circumstances set forth in 5 U.S.C. 552(a)(6)(B)(i) are met. Further, similar to DHS's FOIA regulations at 6 CFR 5.8(a), an appeal must be in writing, and to be considered timely it must be postmarked or, in the case of electronic submissions, transmitted to the Appeals Officer within 90 working days after the date of the component's response. Also, DHS is also making clear in 5.25(a) that any appeal may be directed to either a Component Appeals Officer or to DHS's Office of the General Counsel. The currently regulations only allow an appeal to the Office of the General Counsel or designee. Finally, DHS is proposing to add references to the JRA.

Section 5.26 Requests for Amendment or Correction of Records.

DHS is proposing to amend this section to be consistent with Subpart A. Further, DHS is proposing to add references to the JRA. DHS proposes to note in this section, consistent with the JRA, that for purposes of responding to a JRA amendment request, a covered person is subject to the same limitations, including exemptions and exceptions, as an individual is subject to under section 552a of title 5, United States Code, when pursuing access to records.

Section 5.27 Requests for an Accounting of Record Disclosures.

DHS is proposing to amend this section to make clear that covered persons are not granted any rights under the JRA for requests for an accounting of record disclosures.

Section 5.28 Preservation of Records.

DHS is proposing to amend this section to account for changes made to National Archives and Records Administration's General Records Schedule.

Section 5.29 Fees.

DHS is proposing to amend this section to include references to the JRA. In addition, DHS is proposing to amend this section to make clear that fees for access requests granted in full under the Privacy Act are limited to duplication fees, which are chargeable to the same extent that fees are chargeable under the DHS FOIA regulations. An access request not granted in full under the Privacy Act will be processed under the FOIA and will subject to all fees chargeable under the applicable FOIA regulations.

Section 5.30 Notice of Court-Ordered and Emergency Disclosures.

DHS is proposing to amend this section to provide more detail and further clarification on when Privacy Act protected information may be disclosed pursuant to a court order under subsection 552a(b)(11) of the Privacy Act. Changes to this section are modeled after the Social Security Administration's regulation on disclosures under court order, found at 20 CFR 401.180. *See also 7*2 FR 20935, 20937-38 (Apr. 27, 2007). For instance, this section, as amended, would provide further details on how a court is defined for purposes of this subpart, what conditions must be satisfied to be considered an order to qualify as a court order, how DHS interprets the term "court of competent jurisdiction," and the conditions that must be met for disclosure under a court order of competent jurisdiction. In general, the Privacy Act authorizes the Department to disclose Privacy Act protected information to a third party pursuant to a court order by a court of competent jurisdiction. When information is used in a court proceeding, it usually becomes part of the public record of the proceeding and its confidentiality often cannot

be protected in that record. Much of the information that the component collects and maintains in our records on individuals is especially sensitive. Therefore, the component would follow the conditions and rules in paragraphs (e) through (h) of this section in deciding whether the component may disclose information in response to an order from a court of competent jurisdiction.

Section 5.31 Security of Systems of Records.

DHS proposes no substantives changes to this section.

Section 5.32 Contracts for the Operation of Systems of Records.

DHS proposes to change the title of this section and make minor edits to conform with the statutory language of the Privacy Act.

Section 5.33 Use and Collection of Social Security Numbers.

DHS is proposing to amend this section to account for the passage of the Social Security Number Fraud Prevention Act of 2017, whereby the Department is not permitted to include Social Security numbers of an individual on any document sent by mail unless the Secretary determines that the inclusion of the number on the document is necessary. *See* Pub. L. No. 115-59 (Sept. 15, 2017).

Section 5.34 Standards of Conduct for Administration of the Privacy Act.

DHS is proposing to amend this section, particularly by modifying paragraph (a) to conform to the language in the Privacy Act and by adding paragraph (j) whereby employees would not be permitted to disclose Privacy Act or JRA records unless permitted by 5 U.S.C. 552a(b).

Section 5.35 Sanctions and Penalties.

DHS proposes to amend this section to reference the JRA, and to include the specific Privacy Act provisions that apply for civil remedies and criminal penalties.

Section 5.36 Other Rights and Services.

DHS is proposing to amend this section to reference the JRA.

III. Regulatory Analyses

Executive Orders 12866 and 13563—Regulatory Review

Executive Orders 13563 and 12866 direct agencies to assess the costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). Executive Order 13563 emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. This rule has been designated a "significant regulatory action," under section 3(f) of Executive Order 12866. Accordingly, the rule has been reviewed by the Office of Management and Budget.

DHS has considered the costs and benefits of this proposed rule. Previously in this preamble, DHS has provided a section-by-section analysis of the provisions in this proposed rule and concludes this proposed rule does not impose additional costs on the public or the government. This proposed rule does not collect any additional fee revenues compared to current practices or otherwise introduce new regulatory mandates. The proposed rule's benefits include additional clarity for the public and DHS personnel with respect to DHS's implementation of the Privacy Act and JRA.

Unfunded Mandates Reform Act of 1995

This proposed rule will not result in the expenditure by state, local, and tribal governments, in the aggregate, or by the private sector, of $100,000,000 or more in any one year, and it will not significantly or uniquely affect small governments. Therefore, no written statement was deemed necessary under the provisions of the Unfunded Mandates Reform Act of 1995.

Regulatory Flexibility Act

Under the Regulatory Flexibility Act (RFA), 5 U.S.C. 601-612, and section 213(a) of the Small Business Regulatory Enforcement Fairness Act of 1996, 5 U.S.C. 601 note,

agencies must consider the impact of their rulemakings on "small entities" (small businesses, small organizations and local governments). The term "small entities" comprises small businesses, not-for-profit organizations that are independently owned and operated and are not dominant in their fields, and governmental jurisdictions with populations of less than 50,000. DHS has reviewed this regulation and by approving it certifies that this regulation will not have a significant economic impact on a substantial number of small entities. Based on the previous discussion in this preamble, DHS does not believe this proposed rule imposes any additional direct costs on small entities.

Small Business Regulatory Enforcement Fairness Act of 1996

This rulemaking is not a major proposed rule as defined by section 251 of the Small Business Regulatory Enforcement Fairness Act of 1996 (as amended), 5 U.S.C. 804(2). The Office of Management and Budget's Office of Information and Regulatory Affairs has not found that this proposed rule is likely to result in an annual effect on the economy of $100,000,000 or more; a major increase in costs or prices; or significant adverse effects on competition, employment, investment, productivity, innovation, or on the ability of United States-based companies to compete with foreign-based companies in domestic and export markets.

National Environmental Policy Act

DHS reviews proposed actions to determine whether the National Environmental Policy Act (NEPA) applies to them and, if so, what degree of analysis is required. DHS Directive 023-01 Rev. 01 (Directive) and Instruction Manual 023-01-001-01 Rev. 01 (Instruction Manual) establish the procedures that DHS and its components use to comply with NEPA and the Council on Environmental Quality (CEQ) regulations for implementing NEPA, 40 CFR parts 1500 through 1508.

The CEQ regulations allow federal agencies to establish, with CEQ review and concurrence, categories of actions ("categorical exclusions") which experience has shown

do not individually or cumulatively have a significant effect on the human environment and, therefore, do not require an Environmental Assessment (EA) or Environmental Impact Statement (EIS). 40 CFR 1507.3(b)(2)(ii), 1508.4. For an action to be categorically excluded, it must satisfy each of the following three conditions: (1) the entire action clearly fits within one or more of the categorical exclusions; (2) the action is not a piece of a larger action; and (3) no extraordinary circumstances exist that create the potential for a significant environmental effect. Instruction Manual section V.B(2)(a)-(c).

This proposed rule fits within categorical exclusion A3(a) "Promulgation of rules … of a strictly administrative or procedural nature." Instruction Manual, Appendix A, Table 1. Furthermore, the proposed rule is not part of a larger action and presents no extraordinary circumstances creating the potential for significant environmental impacts. Therefore, the proposed rule is categorically excluded from further NEPA review.

List of Subjects

6 CFR Part 5

Classified Information, Courts, Freedom of information, Government employees, Privacy.

For the reasons stated in the preamble, DHS proposes to amend Chapter I of Title 6, Code of Federal Regulations, as follows:

Title 6 – Domestic Security

PART 5--DISCLOSURE OF RECORDS AND INFORMATION

1. The authority citation for Part 5 is revised to read as follows:

Authority: 6 U.S.C. 101 et seq.; Pub. L. 107-296, 116 Stat. 2135; 5 U.S.C. 301; 6 U.S.C. 142; DHS Del. No. 13001, Rev. 01 (June 2, 2020).

Subpart A also issued under 5 U.S.C. 552.

Subpart B also issued under 5 U.S.C. 552a and 552 note.

§ 5.2 [Amended]

2. In § 5.2, remove the text, “appendix I to this subpart.” and add, in its place, the text “Appendix A to Part 5.”

§ 5.3 [Amended]

3. In § 5.3:

a. In paragraph (a)(1), remove the text, “appendix I of this subpart.” and add, in its place, the text “Appendix A to Part 5.”.

b. In paragraph (b), remove the text, “appendix I of this subpart” and add, in its place, the text “Appendix A to Part 5”.

§ 5.5 [Amended]

4. In § 5.5:

a. In paragraph (a), in the first sentence, remove the text, “Appendix I to this subpart” and add, in its place, the text “Appendix A to Part 5”.

b. In paragraph (e)(2), remove the text “appendix I.” and “appendix I of this subpart.” and add, in both places, the text “Appendix A to Part 5.”

§ 5.8 [Amended]

5. In § 5.8(a)(1), remove the text, “appendix I to this subpart,” and add, in its place, the text “Appendix A to Part 5,”.

6. Revise subpart B of Part 5 to read as follows:

SUBPART B – PRIVACY ACT

Sec.

SUBPART B – PRIVACY ACT

§ 5.20 General Provisions.

(a) *Purpose and scope*. (1) This subpart contains the rules that the Department of Homeland Security (Department or DHS) follows in processing records under the Privacy Act of 1974 (Privacy Act) (5 U.S.C. 552a) and under the Judicial Redress Act of 2015 (JRA) (5 U.S.C. 552a note).

(2) The rules in this subpart should be read in conjunction with the text of the Privacy Act and the JRA, 5 U.S.C. 552a and 5 U.S.C. 552a note, respectively (which provide additional information about records maintained on individuals and covered persons), and JRA designations issued in the *Federal Register*. The rules in this subpart apply to all records in systems of records maintained by the Department. These rules also apply to all records containing Social Security Numbers regardless of whether such records are covered by an applicable system of records maintained by the Department. They describe the procedures by which individuals may request access to records about themselves, request amendment or correction of those records, and request an accounting of disclosures by Department personnel and contractors. In addition, the Department processes all Privacy Act and JRA requests for access to records under the Freedom of Information Act (FOIA) (5 U.S.C. 552), following the rules contained in subpart A of this part, which gives requesters the benefit of both statutes.

(3) The provisions established by this subpart apply to all Department Components, as defined in paragraph (b)(1) of this section.

(4) DHS has a decentralized system for processing requests, with each component handling requests for its records.

(b) *Definitions.* As used in this subpart:

(1) Component means the office that processes Privacy Act and JRA requests for each separate organizational entity within DHS that reports directly to the Office of the Secretary.

(2) Request for access to a record means a request made under Privacy Act subsection (d)(1).

(3) Request for amendment or correction of a record means a request made under Privacy Act subsection (d)(2).

(4) Request for an accounting means a request made under Privacy Act subsection (c)(3).

(5) Requester means an individual who makes a request for access, a request for amendment or correction, or a request for an accounting under the Privacy Act.

(6) Individual means, as defined by the Privacy Act, 5 U.S.C. 552a(a)(2), a citizen of the United States or an alien lawfully admitted for permanent residence. Also, an individual, for purposes of this subpart, but limited to the exclusive rights and civil remedies provided in the JRA, includes covered persons, as defined by the JRA, as a natural person (other than an individual) who is a citizen of a covered country, as designated by the Attorney General, with the concurrence of the Secretary of State, the Secretary of the Treasury, and the Secretary of Homeland Security.

(7) Record has the same meaning as contained in the Privacy Act, 5 U.S.C. 552a(a)(4), except that in cases covered by the JRA, the term “record” has the same meaning as contained in the JRA, 5 U.S.C. 552a note.

(c) *Authority to request records for a law enforcement purpose*. The head of a component or designee thereof is authorized to make written requests under subsection (b)(7) of the

Privacy Act for records maintained by other agencies that are necessary to carry out an authorized law enforcement activity.

(d) *Notice on Departmental use of (b)(1) exception*. As a general matter, when applying the (b)(1) exception for authorized disclosures within an agency on a need to know basis, the Department will consider itself a single entity, meaning that information may be disclosed between components of the Department under the (b)(1) exception.

(e) *Interim Retention of Authorities.* As an interim solution, all agencies and components under the Department will retain the necessary authority from their original purpose in order to conduct these necessary activities. This includes the authority to maintain Privacy Act systems of records, disseminate information pursuant to existing or new routine uses, and retention of exemption authorities under sections (j) and (k) of the Privacy Act, where applicable. This retention of an agency or component's authorities and information practices will remain in effect until this regulation is promulgated as a final rule, or the Department revises all systems of records notices. This retention of authority is necessary to allow components to fulfill their mission and purpose during the transition period of the establishment of the Department. During this transition period, the Department shall evaluate with the components the existing authorities and information practices and determine what revisions (if any) are appropriate and should be made to these existing authorities and practices. The Department anticipates that such revisions will be made either through the issuance of a revised system of records notices or through subsequent final regulations.

§ 5.21 Requests for Access to Records.

(a) *How made and addressed.* (1) DHS has a decentralized system for responding to Privacy Act and JRA requests, with each component designating an office to process records from that component.

(2) An individual may make a request for access to a Department of Homeland Security record about that individual covered by a DHS or Component system of records notice (SORN) by writing directly to the Department component that maintains the record at the address listed in appendix A to this part or via the internet at *http://www.dhs.gov/dhs-foia-request-submission-form*. A description of all DHS-wide and component SORNs may be found here: *https://www.dhs.gov/system-records-notices-sorns*.

(3) In most cases, a component's central FOIA office, as indicated in appendix A to this part, is the place to send a Privacy Act request. For records held by a field office of U.S. Customs and Border Protection, the U.S. Coast Guard, or other Department components with field offices other than the U.S. Secret Service, the requester must write directly to that U.S. Customs and Border Protection, Coast Guard, or other field office address, which can be found by calling the component's central FOIA office. Requests for U.S. Secret Service records should be sent only to the U.S. Secret Service central FOIA office.

(4) Requests for records held by the Cybersecurity and Infrastructure Security Agency (CISA) should be sent to the DHS Privacy Office.

(5) DHS's FOIA Website refers the reader to descriptions of the functions of each component and provides other information that is helpful in determining where to make a request. Each component's FOIA office and any additional requirements for submitting a request to a given component are listed in Appendix A to part 5. These references can all be used by requesters to determine where to send their requests within DHS.

(6) An individual may also send a request to the Privacy Office, Mail Stop 0655, U.S. Department of Homeland Security, 2707 Martin Luther King Jr. Ave. SE, Washington D.C. 20528-0655, or via the internet at *http://www.dhs.gov/dhs-foia-request-submission-form,* or via fax to (202) 343-4011. The Privacy Office will forward the request to the component(s) that it determines to be most likely to maintain the records that are sought.

For the quickest possible handling, the requester should mark both the request letter and the envelope "Privacy Act Request" or "Judicial Redress Act Request."

(b) *Government-wide SORNs.* A government-wide system of records is a system of records where one agency has regulatory authority over records in the custody of multiple agencies, and the agency with regulatory authority publishes a SORN that applies to all of the records regardless of their custodial location. If records are sought that are covered by a Government-wide SORN and requested of DHS, DHS will consult or refer such request, only as applicable and necessary, to the corresponding agency having authority over such records for further processing. DHS will acknowledge to the requester that it is referring the request to another agency or consulting with that agency when processing the request.

(c) *Description of records sought.* A requester must describe the records sought in sufficient detail to enable Department personnel to locate the system of records covering them with a reasonable amount of effort. Whenever possible, the request should describe the records sought, the time periods in which the requester believes they were compiled, the office or location in which the requester believes the records are kept, and the name or identifying number of each system of records in which the requesters believes they are kept. The Department publishes notices in the Federal Register that describe its components' systems of records. These notices can be found on the Department's website here: *https://www.dhs.gov/system-records-notices-sorns*. If a request does not adequately describe the records sought, DHS may at its discretion either administratively close the request or seek additional information from the requester. Requests for clarification or more information will be made in writing (either via U.S. mail or electronic mail whenever possible). Requesters may respond by U.S. Mail or by electronic mail regardless of the method used by DHS to transmit the request for additional information. To be considered timely, responses to requests for additional information must be

postmarked or received by electronic mail within 30 working days of the postmark date or date of the electronic mail request for additional information. If the requester does not respond timely, the request may be administratively closed at DHS's discretion. This administrative closure does not prejudice the requester's ability to submit a new request for further consideration with additional information.

(d) *Agreement to pay fees.* DHS and components shall charge for processing requests under the Privacy Act or JRA. DHS and components will ordinarily use the most efficient and least expensive method for processing requested records. DHS may contact a requester for additional information in order to resolve any fee issues that arise under this section. DHS ordinarily will collect all applicable fees before sending copies of records to a requester. If one makes a Privacy Act or JRA request for access to records, it will be considered a firm commitment to pay all applicable fees charged under section 5.29, up to $25.00. The component responsible for responding to a request ordinarily will confirm this agreement in an acknowledgement letter. When making a request, an individual may specify a willingness to pay a greater or lesser amount. Requesters must pay fees by check or money order made payable to the Treasury of the United States.

(e) *Verification of identity.* When an individual makes a request for access to records about that individual, he or she must verify his or her identity. The individual must state his or her full name, current address, date and place of birth, and country of citizenship or residency. The individual must sign his or her request and provide a signature that must either be notarized or submitted by the requester under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury, as a substitute for notarization. An individual may obtain more information about this process at *http://www.dhs.gov/foia* or 1-866-431-0486. In order to help the identification and location of requested records, an individual may also voluntarily include other identifying information that are relevant to the request (e.g., passport number, Alien Registration Number (A-Number)).

(f) *Verification of guardianship.* When making a request as the parent or guardian of a minor or as the guardian of someone determined by a court of competent jurisdiction to be incompetent due to physical or mental incapacity or age, for access to records about that individual, the individual submitting a request must establish:

(1) The identity of the individual who is the subject of the record, by stating the name, current address, date and place of birth, and country of citizenship or residency of the individual;

(2) The submitting individual's own identity, in the same manner as required in paragraph (e) of this section;

(3) That the submitting individual is the parent or guardian of the subject of the record, which may be proven by providing a copy of the subject of the record's birth certificate showing parentage or by providing a court order establishing guardianship; and

(4) That the submitting individual is acting on behalf of that individual that is the subject of the record.

(g) *Verification in the case of third-party information requests.* Outside of requests made pursuant to paragraph (f) of this section, if a third party requests records about a subject individual, the third party requester must provide verification of the subject individual's identity in the manner provided in paragraph (e) along with the subject individual's written consent authorizing disclosure of the records to the third party requester, or by submitting proof by the requester that the subject individual is deceased (e.g., a copy of a death certificate or an obituary). As an exercise of its administrative discretion, each component can require a third-party requester to supply additional information to verify that the subject individual has consented to disclosure or is deceased.

§ 5.22 Responsibility for Responding to Requests for Access to Records.

(a) *In general.* Except as stated in paragraphs (c), (d), and (e) of this section, the component that first receives a request for access to a record, and has possession of that

record, is the component responsible for responding to the request. In determining which records are responsive to a request, a component ordinarily will include only those records in its possession as of the date the component begins its search for them. If any other date is used, the component will inform the requester of that date.

(b) *Authority to grant or deny requests.* The head of a component, or the component head's designee, is authorized to grant or deny any request for access or amendment to a record of that component.

(c) *Consultations, coordination, and referrals.* All consultations, coordination, and referrals for requests of records subject to the Privacy Act or JRA will follow the same process and procedures as described in 6 CFR 5.4(d), including how to handle those requests that pertain to law enforcement information, as specified in 6 CFR 5.4(d)(2), and classified information, as specified in 6 CFR 5.4(d)(2) and (e). Further, whenever a request is made for access to a record containing information that has been classified by or may be appropriate for classification by another component or agency under any relevant executive order concerning the classification of records, the receiving component will refer to § 5.24 of this Part for processing.

(d) *Release of medical records.* (1) Generally, an individual has the right to access his or her medical records maintained by the Department. Special procedures for requests from an individual who requests his or her medical records that include psychological records for which direct release may cause harm to the individual who is requesting access are set forth in paragraph (d)(2) of this section.

(2) If a request is made for access to medical records that include psychological records, and the component determines that direct release is likely to adversely affect the individual who is requesting access, such that direct release would be reasonably likely to cause harm or endanger physical life or safety of the subject individual or others, the

decision to release records directly to the individual, or to grant indirect release, will be made by a component medical practitioner or other qualified designee. Components will make their best effort to consult the component medical practitioner in the first instance and utilize the qualified designee if the component medical practitioner is unavailable. If the component medical practitioner or qualified designee believes that direct release is likely to adversely affect the individual requesting access, the component will request the individual to provide the name and contact information of a representative who is capable of ameliorating the potential adverse effect. The representative may be a physician, other health professional, or other responsible individual who will be willing to review the record and inform the requester of its contents. Once provided, the component medical practitioner or designee will send the medical records to the individual's designated representative, and the component will inform the subject individual in writing (either via U.S. mail or electronic mail whenever possible) that the record has been sent to that individual's chosen representative. The representative does not have the discretion to withhold any part of your record. If a representative is not provided, the component medical practitioner or designee will discuss such records with the individual first, and will release the records to the individual thereafter.

(e) *Notice of referral.* Whenever a component refers all or any part of the responsibility for responding to a request to another component or agency, it ordinarily will notify the requester of the referral and inform the requester of the name of each component or agency to which the request has been referred and of the part of the request that has been referred.

(f) *Timing of responses to consultations and referrals.* All consultations and referrals received by DHS will be handled according to the date the Privacy Act or JRA access request was initially received by the first component or agency, not any later date.

(g) *Agreements regarding consultations and referrals.* Components may establish agreements with other components or agencies to eliminate the need for consultations or referrals with respect to types of records.

§ 5.23 Responses to Requests for Access to Records.

(a) *In general.* Components should, to the extent practicable, communicate with requesters having access to the Internet using electronic means, such as email or web portal.

(b) *Acknowledgements of requests.* Consistent with the procedures in Subpart A to this Part, a component will acknowledge the request and assign it an individualized tracking number if it will take longer than ten (10) working days to process. Components will include in the acknowledgement a brief description of the records sought to allow requesters to more easily keep track of their requests. Further, in the acknowledgment letter, the component will confirm the requester's agreement to pay fees under 6 CFR 5.21(d) and 5.29.

(c) *Grants of requests for access.* Consistent with the procedures in Subpart A to this Part, a component will have twenty (20) working days from when a request is received to determine whether to grant or deny the request unless there are unusual or exceptional circumstances as defined by the FOIA and set out in 6 CFR 5.5(c). Once a component decides to grant a request for access to record(s) in whole or in part, it will notify the requester in writing. The component will inform the requester in the notice of any fee charged under 6 CFR 5.21(d) and 5.29 and will disclose records to the requester promptly upon payment of any applicable fee. The component will inform the requester of the availability of its FOIA Public Liaison to offer assistance.

(d) *Adverse determinations of requests for access.* A component making an adverse determination denying a request for access in any respect will notify the requester of that determination in writing. Adverse determinations, or denials of requests, include

decisions that: the requested record is exempt, in whole or in part; the requested record does not exist or cannot be located; or the record requested is not subject to the Privacy Act or JRA. Further, adverse determinations also include disputes regarding fees, or denials of a request for expedited processing. The denial letter will be signed by the head of the component, or the component head's designee, and will include:

(1) The name and title or position of the person responsible for the denial;

(2) A brief statement of the reason(s) for the denial, including any Privacy Act exemption(s) applied by the component in denying the request; and

(3) A statement that the denial may be appealed under 6 CFR 5.25(a) and a description of the requirements of 6 CFR 5.25(a).

(e) *JRA access requests.* For purposes of responding to a JRA access request, a covered person is subject to the same limitations, including exemptions and exceptions, as an individual is subject to under section 552a of title 5, United States Code, when pursuing access to records. The implementing regulations and reasons provided for exemptions can be found in Appendix C to 6 CFR part 5, titled DHS Systems of Records Exempt from the Privacy Act.

§ 5.24 Classified Information.

On receipt of any request involving classified information, the component will determine whether information is currently and properly classified and take appropriate action to ensure compliance with 6 CFR part 7. Whenever a request is made for access to a record that is covered by a system of records containing information that has been classified by or may be appropriate for classification by another component or agency under any applicable executive order, the receiving component will consult the component or agency that classified the information. Whenever a record contains information that has been derivatively classified by a component or agency because it contains information classified by another component or agency, the component will consult the component or

agency that classified the underlying information. Information determined to no longer require classification will not be withheld from a requester based on exemption (k)(1) of the Privacy Act. On receipt of any appeal involving classified information, the DHS Office of the General Counsel or its designee, shall take appropriate action to ensure compliance with part 7 of this title.

§ 5.25 Administrative Appeals for Access Requests.

(a) *Requirements for filing an appeal.* An individual may appeal an adverse determination denying his or her request for access in any respect to the appropriate component Appeals Officer. For the address of the appropriate component Appeals Officer, an individual may contact the applicable component FOIA Requester Service Center or FOIA Public Liaison using the information in appendix A to Part 5, visit *www.dhs.gov/foia,* or call 1-866-431-0486. Alternatively, an individual may also appeal to the DHS Office of the General Counsel or its designee in writing, by mail or email indicated here *https://www.dhs.gov/office-general-counsel*. An appeal must be in writing, and to be considered timely it must be postmarked or, in the case of electronic submissions, transmitted to the Appeals Officer within 90 working days, consistent with the procedures in Subpart A to this Part, after the date of the component's response . An electronically filed appeal will be considered timely if transmitted to the Appeals Officer by 11:59:59 p.m. EST. The appeal should clearly identify the component determination (including the assigned request number if the requester knows it) that is being appealed and should contain the reasons the requester believes the determination was erroneous. For the quickest possible handling, an individual should mark both his or her appeal letter and the envelope "Privacy Act Appeal" or "Judicial Redress Act Appeal."

(b) *Adjudication of appeals.* The DHS Office of the General Counsel or its designee (e.g., Component Appeals Officers) is the authorized appeals authority for DHS. On receipt of any appeal involving classified information, the Appeals Officer will consult with the

Chief Security Officer and take appropriate action to ensure compliance with 6 CFR Part 7. If the appeal becomes the subject of a lawsuit, the Appeals Officer is not required to act further on the appeal.

(c) *Appeal decisions.* Consistent with the procedures in Subpart A to this Part, the decision on an appeal will be made in writing generally twenty (20) working days after receipt. However, consistent with the procedures in Subpart A to this Part, the time limit for responding to an appeal may be extended provided the circumstances set forth in 5 U.S.C. 552(a)(6)(B)(i) are met. A decision affirming an adverse determination in whole or in part will include a brief statement of the reason(s) for the affirmance, including any Privacy Act exemption applied, and will inform the requester of the Privacy Act provisions for court review of the decision. If the adverse determination is reversed or modified on appeal in whole or in part, the requester will be notified in a written decision and his or her request will be reprocessed in accordance with that appeal decision. An adverse determination by the DHS Office of the General Counsel or its designee or Component Appeals Officer will be the final action of the Department.

(d) *Appeal necessary before seeking court review.* If an individual wishes to seek review by a court of any adverse determination or denial of a request by DHS within the allotted 20 working days to respond unless there are unusual or exceptional circumstances, that individual must first appeal it under this subpart. An appeal will not be acted on if the request becomes a matter of litigation.

§ 5.26 Requests for Amendment or Correction of Records.

(a) *How made and addressed.* Unless the record is not subject to amendment or correction as stated in paragraph (f) of this section, an individual may make a request for amendment or correction of a record of the Department about that individual by writing directly to the component that maintains the record, following the procedures in section 5.21. The request should identify each record in question, state the amendment or

correction requested, and state the reason why the requester believes that the record is not accurate, relevant, timely, or complete. The requester may submit any documentation that he or she thinks would support his or her request. If the individual believes that the same record is in more than one system of records, he or she should state that and address his or her request to each component that maintains a system of records containing the record.

(b) *Component responses.* Within ten working days of receiving a request for amendment or correction of records, a component will send the requester a written acknowledgment of its receipt of the request, and it will promptly notify the requester whether the request is granted or denied. If the component grants the request in whole or in part, it will describe the amendment or correction made and will advise the requester of his or her right to obtain a copy of the corrected or amended record, in disclosable form. If the component denies the request in whole or in part, it will send the requester a letter signed by the head of the component, or the component head's designee, that will state:

(1) The reason(s) for the denial; and

(2) The procedure for appeal of the denial under paragraph (c) of this section, including the name and business address of the official who will act on his or her appeal.

(c) *Appeals.* Within 90 working days after the date of the component's response, the requester may appeal a denial of a request for amendment or correction to the Component Appeals Officer or the DHS Office of the General Counsel or its designee. The Component Appeals Officer or the DHS Office of the General Counsel or its designee must complete its review and make a final determination on the requester's appeal no later than 30 days (excluding Saturdays, Sundays, and legal public holidays) from the date on which the individual requests such review unless good cause is shown, and communicated to the individual, for which the 30-day period may be extended for an additional 30 days. If the appeal is denied, the requester will be advised of his or her right

to file a Statement of Disagreement as described in paragraph (d) of this section and of his or her right under the Privacy Act, 5 U.S.C. 552a(d)(3), for court review of the decision. If an individual wishes to seek review by a court of any adverse determination or denial of a request, that individual must first appeal it under this subpart. For purposes of responding to a JRA amendment request, a covered person is subject to the same limitations, including exemptions and exceptions, as an individual is subject to under section 552a of title 5, United States Code, when pursuing amendment to records. The implementing regulations and reasons provided for exemptions can be found in Appendix C to 6 CFR part 5, titled DHS Systems of Records Exempt from the Privacy Act.

(d) *Statements of Disagreement.* If an individual's appeal under this section is denied in whole or in part, that individual has the right to file a Statement of Disagreement, unless exempt, that states his or her reason(s) for disagreeing with the Department's denial of his or her request for amendment or correction. Statements of Disagreement must be concise, must clearly identify each part of any record that is disputed, and should be no longer than one typed page for each fact disputed. The individual's Statement of Disagreement must be sent to the component involved, which will place it in the system of records in which the disputed record is maintained and will mark the disputed record to indicate that a Statement of Disagreement has been filed and where in the system of records it may be found.

(e) *Notification of amendment/correction or disagreement.* Within 30 working days of the amendment or correction of a record, the component that maintains the record will, unless exempt, notify all persons, organizations, or agencies to which it previously disclosed the record, if an accounting of that disclosure was made or should have been made, that the record has been amended or corrected. If an individual has filed a Statement of Disagreement, the component will append a copy of it to the disputed record

whenever the record is disclosed and may also append a concise statement of its reason(s) for denying the request to amend or correct the record.

(f) *Records not subject to amendment or correction.* The following records are not subject to amendment or correction:

(1) Transcripts of testimony given under oath or written statements made under oath;

(2) Transcripts of grand jury proceedings, judicial proceedings, or quasi-judicial proceedings, which are the official record of those proceedings;

(3) Presentence records that originated with the courts; and

(4) Records in systems of records that have been exempted from amendment and correction under the Privacy Act (5 U.S.C. 552a(j) or (k)) pursuant to a Final Rule published in the *Federal Register*.

§ 5.27 Requests for an Accounting of Record Disclosures.

(a) *How made and addressed.* Except where accountings of disclosures are not required to be kept (as stated in paragraph (b)(1) of this section), an individual may make a request for an accounting of any disclosure that has been made by the Department to another person, organization, or agency of any record about the requester, except to the extent the records are covered by the JRA. This accounting contains the date, nature, and purpose of each disclosure, as well as the name and address of the person, organization, or agency to which the disclosure was made. A request for an accounting should identify each record in question and should be made by writing directly to the Department component that maintains the record, following the procedures in section 5.21.

(b) *Where accountings are not required.* Components are not required to provide accountings to the requester where they relate to:

(1) Disclosures for which accountings are, by statute (5 U.S.C. 552a(c)(1)), not required to be kept, such as disclosures that are made to officers and employees within the agency and disclosures that are required to be made under the FOIA;

(2) Disclosures made to law enforcement agencies for authorized law enforcement activities in response to written requests from those law enforcement agencies specifying the law enforcement activities for which the disclosures are sought; or

(3) Disclosures made from systems of records that have been exempted from accounting requirements by a rulemaking pursuant to 5 U.S.C. 552a(j) or (k).

(c) *Appeals.* A requester may appeal a denial of a request for an accounting to the Component Appeals Officer or the DHS Office of the General Counsel or its designee in the same manner as a denial of a request for access to records (see § 5.25 of this part) and the same procedures will be followed.

§ 5.28 Preservation of Records.

Each component will preserve all correspondence pertaining to the requests that it receives under this subpart, as well as copies of all requested records, until disposition or destruction is authorized by title 44 of the United States Code or the National Archives and Records Administration's General Records Schedule 4.2. Records will not be disposed of while they are the subject of a pending request, appeal, lawsuit, or litigation or audit hold under the Act.

§ 5.29 Fees.

(a) Fees for access requests granted in full under the Privacy Act are limited to duplication fees, which are chargeable to the same extent that fees are chargeable under the 6 CFR part 5, subpart A. An access request not granted in full under the Privacy Act will be processed under the FOIA and will subject to all fees chargeable under the applicable FOIA regulations. Fees are not charged for processing amendment and accounting requests.

(b) DHS will not process a request under the Privacy Act or JRA from persons with an unpaid fee from any previous Privacy Act or JRA request to any Federal agency until that outstanding fee has been paid in full to the agency.

§ 5.30 Notice of Court-Ordered and Emergency Disclosures.

(a) *Court-ordered disclosures.* When the component discloses an individual's information covered by a system of records pursuant to an order from a court of competent jurisdiction, and the order is a matter of public record, the Privacy Act requires the component to send a notice of the disclosure to the last known address of the person whose record was disclosed. Notice will be given within a reasonable time after the component's receipt of the order, except that in a case in which the order is not a matter of public record, the notice will be given only after the order becomes public. This notice will be mailed to the individual's last known address and will contain a copy of the order and a description of the information disclosed. Notice will not be given if disclosure is made from a criminal law enforcement system of records that has been exempted from the notice requirement.

(b) *Court.* For purposes of this section, a court is an institution of the judicial branch of the U.S. Federal Government consisting of one or more judges who seek to adjudicate disputes and administer justice. Entities not in the judicial branch of the Federal Government are not courts for purposes of this section.

(c) *Court order.* For purposes of this section, a court order is any legal process which satisfies all the following conditions:

(1) It is issued under the authority of a Federal court;

(2) A judge or a magistrate judge of that court signs it;

(3) It commands or permits DHS to disclose the Privacy Act protected information at issue; and

(4) The court is a court of competent jurisdiction.

(d) *Court of competent jurisdiction.* It is the view of DHS that under the Privacy Act the Federal Government has not waived sovereign immunity, which precludes state court

jurisdiction over a Federal agency or official. Therefore, DHS will not honor state court orders as a basis for disclosure, unless DHS does so under its own discretion.

(e) *Conditions for disclosure under a court order of competent jurisdiction.* The component may disclose information in compliance with an order of a court of competent jurisdiction if—

(1) Another section of this part specifically allows such disclosure, or

(2) DHS, the Secretary, or any officer or employee of DHS in his or her official capacity is properly a party in the proceeding, or

(3) Disclosure of the information is necessary to ensure that an individual who is accused of criminal activity receives due process of law in a criminal proceeding under the jurisdiction of the judicial branch of the Federal Government.

(f) *In other circumstances.* DHS may disclose information to a court of competent jurisdiction in circumstances other than those stated in paragraph (e) of this section. DHS will make its decision regarding disclosure by balancing the needs of a court while preserving the confidentiality of information. For example, DHS may disclose information under a court order that restricts the use and redisclosure of the information by the participants in the proceeding; DHS may offer the information for inspection by the court *in camera* and under seal; or DHS may arrange for the court to exclude information identifying individuals from that portion of the record of the proceedings that is available to the public.

(g) *Emergency disclosures*. Upon disclosing a record pertaining to an individual made under compelling circumstances affecting the health or safety of an individual, the component will notify the individual to whom the record pertains of the disclosure. This notice will be mailed to the individual's last known address and will state the nature of the information disclosed; the person, organization, or agency to which it was disclosed; the date of disclosure; and the compelling circumstances justifying the disclosure.

(h) *Other regulations on disclosure of information in litigation.* See 6 CFR part 5, subpart C, for additional rules covering disclosure of information and records governed by this part and requested in connection with legal proceedings.

§ 5.31 Security of Systems of Records.

(a) *In general.* Each component will establish administrative and physical controls to prevent unauthorized access to its systems of records, to prevent unauthorized disclosure of records, and to prevent physical damage to or destruction of records. The stringency of these controls will correspond to the sensitivity of the records that the controls protect. At a minimum, each component's administrative and physical controls will ensure that:

(1) Records are protected from public view;

(2) The area in which records are kept is supervised during business hours to prevent unauthorized persons from having access to them;

(3) Records are inaccessible to unauthorized persons outside of business hours; and

(4) Records are not disclosed to unauthorized persons or under unauthorized circumstances in either oral or written form.

(b) *Procedures required.* Each component will have procedures that restrict access to records to only those individuals within the Department who must have access to those records to perform their duties and that prevent inadvertent disclosure of records.

§ 5.32 Contracts for the Operation of Systems of Records.

As required by 5 U.S.C. 552a(m), any approved contract for the operation of a system of records to accomplish an agency function will contain the standard contract requirements issued by the General Services Administration to ensure compliance with the requirements of the Privacy Act for that system. The contracting component will be responsible for ensuring that the contractor complies with these contract requirements.

§ 5.33 Use and Collection of Social Security Numbers.

Each component will ensure that employees authorized to collect information are aware:

(a) That individuals may not be denied any right, benefit, or privilege because of refusing to provide their Social Security numbers, unless the collection is authorized either by a statute or by a regulation issued prior to 1975; and

(b) That individuals requested to provide their Social Security numbers must be informed of:

(1) Whether providing Social Security numbers is mandatory or voluntary;

(2) Any statutory or regulatory authority that authorizes the collection of Social Security numbers; and

(3) The uses that will be made of the numbers.

(c) Including Social Security numbers of an individual on any document sent by mail is not permitted unless the Secretary determines that the inclusion of the number on the document is necessary.

§ 5.34 Standards of Conduct for Administration of the Privacy Act.

Each component will inform its employees of the provisions of the Privacy Act, including the Act's civil liability and criminal penalty provisions referenced in §5.35. Unless otherwise permitted by law, the Department will:

(a) Maintain only such information about an individual as is relevant and necessary to accomplish a purpose of the Component or the Department that is required to be accomplished by statute or by executive order of the President;

(b) Collect information about an individual directly from that individual whenever practicable and when the information may result in adverse determinations about an individual's rights, benefits, and privileges under federal programs;

(c) Inform each individual from whom information is collected of:

(1) The legal authority to collect the information and whether providing it is mandatory or voluntary;

(2) The principal purpose for which the Department intends to use the information;

(3) The routine uses the Department may make of the information; and

(4) The effects on the individual, if any, of not providing the information;

(d) Ensure that the component maintains no system of records without public notice and that it notifies appropriate Department officials of the existence or development of any system of records that is not the subject of a current or planned public notice;

(e) Maintain all records that are used by the Department in making any determination about an individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual in the determination;

(f) Except as to disclosures made to an agency or made under the FOIA, make reasonable efforts, prior to disseminating any record about an individual, to ensure that the record is accurate, relevant, timely, and complete;

(g) Maintain no record describing how an individual exercises his or her First Amendment rights, unless it is expressly authorized by statute or by the individual about whom the record is maintained, or is pertinent to and within the scope of an authorized law enforcement activity;

(h) When required by the Act, maintain an accounting in the specified form of all disclosures of records by the Department to persons, organizations, or agencies;

(i) Maintain and use records with care to prevent the unauthorized or inadvertent disclosure of a record to anyone; and

(j) Disclose Privacy Act or JRA records only as permitted by 5 U.S.C. 552a(b).

§ 5.35 Sanctions and Penalties.

Each component will inform its employees and contractors of the Privacy Act's civil liability provisions (5 U.S.C. 552a(g)) and criminal penalty provisions (5 U.S.C. 552a(i)) as they apply to Privacy Act and JRA complaints.

§ 5.36 Other Rights and Services.

Nothing in this subpart will be construed to entitle any person, as of right, to any service

or to the disclosure of any record to which such person is not entitled under the Privacy Act or JRA.

7. Revise Appendix A to Part 5 to read as follows:

Appendix A to Part 5 – FOIA/Privacy Act Offices of the Department of Homeland Security

I. For the following Headquarters Offices of the Department of Homeland Security, FOIA and Privacy Act requests should be sent to the Department's Privacy Office, Mail Stop 0655, U.S. Department of Homeland Security, 2707 Martin Luther King Jr. Ave. SE, Washington D.C. 20528-0655, Phone: 202-343-1743 or 866-431-0486, Fax: 202-343-4011, Email: *foia@hq.dhs.gov*. The Headquarters Offices are:

Office of the Secretary

Office of the Deputy Secretary

Office of the General Counsel (OGC)

Office of the Executive Secretary (ESEC)

Office of Intelligence and Analysis (I&A)

Office of Legislative Affairs (OLA)

Office of Operations Coordination (OPS)

Office of Partnership and Engagement (OPE)

Office of Public Affairs (OPA)

Office of Strategy, Policy, and Plans (PLCY)

Citizenship and Immigration Services Ombudsman (CISOMB)

Civil Rights and Civil Liberties (CRCL)

Countering Weapons of Mass Destruction Office (CWMD)

Federal Protective Service (FPS)

Management Directorate (MGMT), including the Office of Biometric Identity

Management (OBIM)

Military Advisor's Office (MIL)

Privacy Office (PRIV)

Science and Technology Directorate (S&T)

II. For the following components and Offices of the Department of Homeland Security, FOIA and Privacy Act requests should be sent to the component's FOIA Office, unless otherwise noted below. The components are:

Cybersecurity and Infrastructure Security Agency (CISA)

All requests should be sent to the Department's Privacy Office, Mail Stop 0655, U.S. Department of Homeland Security, 2707 Martin Luther King Jr. Ave. SE, Washington D.C. 20528-0655, Phone: 202-343-1743 or 866-431-0486, Fax: 202-343-4011, Email: *foia@hq.dhs.gov*

Customs and Border Protection (CBP)

All requests should be sent to U.S. Customs and Border Protection, 1300 Pennsylvania Avenue, Washington, DC 20004-3002

Phone: 202-325-0150

https://foiaonline.gov/foiaonline/action/public/home

Federal Emergency Management Agency (FEMA)

All requests should be sent to FOIA Officer, 500 C Street, S.W., Room 840, Washington, D.C. 20472, Phone: 202-646-3323, Fax: 202-646-3347, E-mail: fema-foia@fema.dhs.gov

Federal Law Enforcement Training Center (FLETC)

All requests should be sent to Freedom of Information Act Officer, Building #681, Suite B187, 1131 Chapel Crossing Road, Glico, GA 31524, Phone: 912-267-3103, Fax: 912-267-3113, E-mail: fletc-foia@dhs.gov

Immigration and Customs Enforcement (ICE)

All requests should be sent to Freedom of Information Act Office, 500 12th Street, SW, Stop 5009, Washington, D.C. 20536-5009, Phone: 866-633-1182, Fax: 202-732-4265, E-mail: ice-foia@dhs.gov

Office of Inspector General

All requests should be sent to the OIG Office of Counsel, 245 Murray Lane SW, Mail Stop – 0305, Washington, D.C. 20528-0305, Phone: 202-981-6100, Fax: 202-245-5217; E-mail: foia.oig@oig.dhs.gov

Transportation Security Administration (TSA)

All requests should be sent to Freedom of Information Act Branch, 601 S. 12th Street, 3rd Floor, West Tower, TSA-20, Arlington, VA 20598-6020, Phone: 1-866-FOIA-TSA or 571-227-2300, Fax: 571-227-1406, E-mail: foia@tsa.dhs.gov

U.S. Citizenship and Immigration Services (USCIS)

All requests should be sent to National Records Center, FOIA/PA Office, P. O. Box 648010, Lee's Summit, MO. 64064-8010 or through the USCIS FOIA Portal: https://first.uscis.gov/; General questions may be posed either through Phone (1-800-375-5283 - USCIS Contact Center) or by E-mail (uscis.foia@uscis.dhs.gov)

U.S. Coast Guard (USCG)

All requests should be sent to Commandant (CG-611), 2701 Martin Luther King Jr. Ave., SE, Stop 7710, Washington, DC 20593-7710, Phone: 202-475-3522, Fax: 202-372-8413, E-mail: efoia@uscg.mil

U.S. Secret Service (USSS)

All requests should be sent to Freedom of Information Act and Privacy Act Branch, 245 Murray Lane, SW Building T-5, Washington, D.C. 20223, Phone: 202-406-6370, Fax: 202-406-5586, E-mail: FOIA@usss.dhs.gov

Lynn Parker Dupree,
Chief Privacy Officer,
Department of Homeland Security.

[FR Doc. 2021-21374 Filed: 10/5/2021 8:45 am; Publication Date: 10/6/2021]