



BILLING CODE 4410-PJ

## **DEPARTMENT OF JUSTICE**

### **28 CFR Part 16**

**[CPCLO Order No. 12-2021; AG Order No. 5851-2024]**

**RIN 1105-AB66**

### **Privacy Act Regulations**

**AGENCY:** United States Department of Justice.

**ACTION:** Final rule.

**SUMMARY:** This rule amends the United States Department of Justice (“DOJ” or “Department”) Privacy Act implementation regulations, including its Privacy Act record access and amendment procedures. Additionally, this rule includes procedures regarding processing Privacy Act requests to access or amend covered records, as designated under the Judicial Redress Act of 2015, and expands protections on the Department’s maintenance of Social Security account numbers, in accordance with the Social Security Number Fraud Prevention Act of 2017.

**DATES:** This final rule is effective **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

**FOR FURTHER INFORMATION CONTACT:** Katherine Harman-Stokes, Acting Director, U.S. Department of Justice, Office of Privacy and Civil Liberties, Two Constitution Square, 145 N Street, NE, Suite 8W.300, Washington, DC 20530, telephone (202) 514-0208 (not a toll-free call).

### **SUPPLEMENTARY INFORMATION:**

#### **I. Public Participation**

The Department received no comments in response to the notice of proposed rulemaking for the revision of the Department of Justice Privacy Act regulations published on January 6, 2023, 88 FR 1012, and now finalizes this rule without changes.

## **II. Overview of the Department’s Privacy Act of 1974 Implementation Regulations**

The Privacy Act of 1974, as amended, 5 U.S.C. 552a (“Privacy Act”), establishes certain agency responsibilities and individual rights regarding the collection, use, maintenance, and disclosure of records about individuals. To carry out these rights, the Privacy Act requires agencies to promulgate rules that will: (1) establish procedures whereby an individual can be notified if any system of records named by the individual contains a record pertaining to that individual; (2) define reasonable times, places, and requirements for identifying an individual who requests a record or information pertaining to the individual before the agency shall make the record or information available; (3) establish procedures for the disclosure to an individual upon request of a record or information pertaining to the individual, including special procedures, if deemed necessary, for the disclosure to an individual of medical records pertaining to the individual; (4) establish procedures for reviewing a request from an individual concerning the amendment of any record or information pertaining to the individual, for making a determination on the request, for an appeal within the agency of an initial adverse agency determination, and for whatever additional means may be necessary for each individual to exercise fully the individual’s rights under the Privacy Act; and (5) establish fees to be charged, if any, to any individual for making copies of records pertaining to the individual, excluding the cost of any search for and review of the record. 5 U.S.C. 552a(f).

The Department's Privacy Act regulations are promulgated at title 28, part 16, subpart D, Code of Federal Regulations. While existing procedures have largely remained the same, certain amendments are required to ensure the Department's Privacy Act regulations reflect changes in the law, as well as in the Department's practices.

### **III. Discussion of Changes**

#### **A. Relationship to the Freedom of Information Act**

The Department continues to process all Privacy Act 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 part 16, thus giving requesters the benefit of both statutes. The updates to subpart D, in particular 28 CFR 16.41 through 16.45, better align the FOIA and Privacy Act request-for-access procedures. For example, updates to 28 CFR 16.42 align the consultation, referral, and coordination procedures with the FOIA procedures under 28 CFR 16.4, subject to certain deviations to comply with Privacy Act requirements. Updates to 28 CFR 16.42 through 16.43 align the re-routing of misdirected Privacy Act requests for access procedures, the procedures for determining which component is responsible for responding to a request, and the timing for those responses, with the FOIA procedures contained in 28 CFR part 16, subpart A. Finally, similar to the FOIA procedures, components are encouraged, to the extent practicable, to communicate with requesters having access to the Internet using electronic means, such as by email or through a web portal.

#### **B. Updates to the Privacy Act Request-for-Access Procedures**

The changes set forth in this rule update the Department's Privacy Act request-for-access procedures to more accurately reflect existing practices. First, the rules clarify

that the Department has a decentralized system for responding to Privacy Act requests for access, by informing requesters that they may make a Privacy Act request for access by writing directly to the component that maintains the record. 28 CFR 16.41(a)(1). The updates remove the requirement that a requester send or deliver requests to Department field offices, and instead requires requesters to send or deliver requests to the component's office at the address listed in appendix I to 28 CFR part 16, or in accordance with the access procedures outlined in the corresponding System of Records Notice. 28 CFR 16.41(a)(2).

Additionally, the updates remove explicit references to in-person Privacy Act requests for access because such requests have become generally impracticable for members of the public. That said, the new procedures explicitly state that a requester may request a record in a particular form or format, 28 CFR 16.41(b), and components will honor a requester's preference where the record is readily reproducible by the component in the form or format requested, 28 CFR 16.43(a). This would continue to permit a member of the public to request access to the member's records in-person when components can provide a copy of the record for in-person inspection.

#### C. Updates to the Privacy Act Procedures for Requests for Amendment or Correction

The rule updates the Department's procedures for requesting amendment or correction of records under the Privacy Act, in accordance with existing practices. First, the rule would explicitly set out the timing for components to respond to a Privacy Act request for amendment or correction. 28 CFR 16.46(b). In accordance with the Privacy Act, 5 U.S.C. 552a(d)(2), components responsible for responding to a Privacy Act request for amendment or correction must acknowledge, in writing, the receipt of the

request no later than ten (10) working days after receipt, and must promptly grant or refuse to grant the request. 28 CFR 16.46(b)(1). The rule authorizes components to designate multiple processing tracks that distinguish between simple and more complex Privacy Act requests for amendment or correction, consistent with the Privacy Act request-for-access procedures. 28 CFR 16.46(b)(3). The rule requires components to provide additional content in the response that components must provide when refusing to grant a Privacy Act request for amendment or correction. 28 CFR 16.46(e). Finally, the rule updates the list of records not subject to amendment or correction. 28 CFR 16.46(i).

#### D. Privacy Act Access Appeals and Privacy Act Amendment Appeals

The rule updates the Department's Privacy Act administrative appeal procedures to align with existing practices. First, the rules clarify that a refusal to grant a Privacy Act request for access or Privacy Act request for amendment or correction is subject to an administrative appeal, and provides examples of what commonly qualifies as a refusal to grant a Privacy Act request. 28 CFR 16.45 through 16.46. The rule clarifies that the Attorney General has designated the Director of the Office of Information Policy, or the Director's designee, with the responsibility for adjudicating Privacy Act access appeals, 28 CFR 16.45(b)(1), and the DOJ Chief Privacy and Civil Liberties Officer ("CPCLO"), or the CPCLO's designee, with the responsibility for adjudicating Privacy Act amendment appeals. 28 CFR 16.46(f)(1).

#### E. Safeguards and Employee Code of Conduct

The rule updates the Department's Privacy Act record safeguard requirements and employee conduct requirements to reflect updated standards of practice. First, the

updates clarify that the Department’s administrative, technical, and physical controls in place for its systems of records are consistent with applicable Department and government-wide laws, regulations, policies, and standards, including but not limited to those required for the security of Department information systems. 28 CFR 16.51.

Second, the updates require Department employees to read, acknowledge, and agree to abide by the Department of Justice rules of behavior for accessing, collecting, using, maintaining, and protecting personally identifiable information. 28 CFR 16.54.

#### F. Judicial Redress Act of 2015

The Judicial Redress Act of 2015, Public Law 114-126, 130 Stat. 282 (“Judicial Redress Act”), codified at 5 U.S.C. 552a note, extends certain rights of judicial redress established under the Privacy Act to citizens of foreign countries or regional economic organizations certified as a “covered country.” Specifically, the Judicial Redress Act enables a “covered person” (i.e., a natural person, other than a U.S. citizen or permanent resident alien, who is a citizen of a covered country) to bring suit and obtain specified redress 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 permanent resident alien) may bring suit and obtain specified redress with respect to the improper refusal to grant access to or an amendment of a “covered record” (i.e., a record pertaining to the covered person transferred by a public authority of, or a private entity within, a covered country to a designated Federal agency or component for purposes of preventing, investigating, detecting, or prosecuting criminal offenses) under 5 U.S.C. 552a(g)(1)(A) & (B). The updates clarify that, consistent with the processes established for individuals under the Privacy Act, a covered person must follow the Privacy Act request-for-access

procedures, or the Privacy Act request-for-amendment or correction procedures, before a covered person may file suit. 28 CFR 16.40(e).

#### G. Social Security Number Fraud Prevention Act of 2017

The Social Security Number Fraud Prevention Act of 2017, Public Law 115-59, 131 Stat. 1152 (“SSN Fraud Prevention Act”), codified at 42 U.S.C. 405 note, requires the Department to promulgate rules that will: (1) specify the circumstances under which inclusion of a Social Security account number on a document sent by mail is necessary; (2) instruct components on the partial redaction of Social Security account numbers where feasible; and (3) require that Social Security account numbers not be visible on the outside of any package sent by mail. This proposal promulgates the above requirements.

Specifically, the updates define the term “necessary” to include only those circumstances in which a component would be unable to comply, in whole or in part, with a legal, regulatory, or policy requirement if prohibited from mailing the full Social Security account number. 28 CFR 16.53(b). The definition further specifies that including the full Social Security account number on a document sent by mail is not necessary if a legal, regulatory, or policy requirement could be satisfied by either partially redacting the Social Security account number or by removing the Social Security number entirely. *Id.* Components are then restricted from including the full Social Security account number on any document sent by mail unless the inclusion of the Social Security account number on the document is necessary. 28 CFR 16.53(d). Unless the Attorney General directs otherwise, the CPCLO is authorized to assist components in interpreting this paragraph. 28 CFR 16.53(d)(1).

The updates also instruct components, where feasible, to partially redact the Social Security account number on any document sent by mail by including no more than the last four digits of the Social Security account number, while prioritizing technical methods to facilitate such redactions. 28 CFR 16.53(d)(3).

#### H. Administrative Amendments

Finally, the rule amends 28 CFR part 16, subpart D, throughout to correct minor administrative edits or to reorganize sentences, sections, or paragraphs for readability.

### **IV. Regulatory Certifications**

#### **Executive Orders 12866 and 13563—Regulatory Review**

This rule does not raise novel legal or policy issues, nor does it adversely affect the economy, the budgetary impact of entitlements, grants, user fees, loan programs, or the rights and obligations of recipients thereof in a material way. The Department of Justice has determined that this rule is not a “significant regulatory action” under Executive Order 12866, section 3(f), and accordingly this rule has not been reviewed by the Office of Information and Regulatory Affairs within the Office of Management and Budget (“OMB”) pursuant to Executive Order 12866.

#### **Regulatory Flexibility Act**

This rule relates to individuals rather than small business entities. Pursuant to the requirements of the Regulatory Flexibility Act of 1980, 5 U.S.C. 601-612, therefore, the rule will not have a significant economic impact on a substantial number of small entities.

#### **Congressional Review Act**

This rule is not a major rule as defined by the Congressional Review Act, 5 U.S.C. 804. This rule will not 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.

### **Paperwork Reduction Act**

The Paperwork Reduction Act of 1995, 44 U.S.C. 3507(d), requires the Department to consider the impact of paperwork and other information collection burdens imposed on the public. The DOJ Certification of Identity Form, DOJ-361, has been assigned OMB No. 1103-0016.

### **Unfunded Mandates Reform Act of 1995**

This 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 actions were deemed necessary under the provisions of the Unfunded Mandates Reform Act of 1995.

### **Executive Order 13132–Federalism**

This rule will not have substantial direct effects on the States, on the relationship between the National Government and the States, or on distribution of power and responsibilities among the various levels of government. Therefore, in accordance with Executive Order 13132, it is determined that this rule does not have sufficient federalism implications to warrant the preparation of a Federalism Assessment.

### **Executive Order 12988–Civil Justice Reform**

This rule meets the applicable standards set forth in sections 3(a) and 3(b)(2) of Executive Order 12988 to eliminate drafting errors and ambiguity, minimize litigation,

provide a clear legal standard for affected conduct, and promote simplification and burden reduction.

### **Executive Order 13175–Consultation and Coordination With Indian Tribal Governments**

This rule will have no implications for Indian Tribal governments. More specifically, it does not have substantial direct effects on one or more Indian tribes, on the relationship between the Federal Government and Indian tribes, or on the distribution of power and responsibilities between the Federal Government and Indian tribes. Therefore, the consultation requirements of Executive Order 13175 do not apply.

### **List of Subjects in 28 CFR Part 16**

Administrative practices and procedures, Courts, Freedom of information, Privacy.

Pursuant to the authority vested in me by 5 U.S.C. 552a and 42 U.S.C. 405 note, the Department of Justice amends 28 CFR part 16 as follows:

### **PART 16-PRODUCTION OR DISCLOSURE OF MATERIAL OR INFORMATION**

1. The authority citation for part 16 is revised to read as follows:

**Authority:** 5 U.S.C. 301, 552, 552a, 553; 28 U.S.C. 509, 510, 534; 31 U.S.C. 3717; 42 U.S.C. 405.

2. Revise subpart D to read as follows:

### **Subpart D - Access to and Amendment of Individual Records Pursuant to the Privacy Act of 1974, and Other Privacy Protections**

Sec.

- 16.40 General provisions.
- 16.41 Privacy Act requests for access to records.
- 16.42 Responsibility for responding to Privacy Act requests for access to records.
- 16.43 Responses to Privacy Act requests for access to records.
- 16.44 Classified information.
- 16.45 Privacy Act access appeals.
- 16.46 Privacy Act requests for amendment or correction.
- 16.47 Privacy Act requests for an accounting of record disclosures.
- 16.48 Preservation of records.
- 16.49 Fees.
- 16.50 Notice of compulsory legal process and emergency disclosures.
- 16.51 Security of systems of records.
- 16.52 Contracts for the operation of record systems.
- 16.53 Use and collection of Social Security account numbers.
- 16.54 Employee standards of conduct.
- 16.55 Other rights and services.

**§ 16.40 General provisions.**

(a) *Purpose and scope.* (1) This subpart contains the rules that the Department of Justice (“DOJ” or “the Department”) follows when handling records maintained by the Department in a system of records, in accordance with the Privacy Act of 1974, as amended, 5 U.S.C. 552a (“Privacy Act” or “PA”). This subpart describes the procedures by which individuals can be notified if a Department system of records contains records about themselves, may request access to records about themselves maintained in a

Department system of records, may request amendment or correction of records about themselves maintained in a Department system of records, and may request an accounting of disclosures of records about themselves maintained in a Department system of records. This subpart also establishes other procedures on the appropriate maintenance of records by the Department and when Privacy Act exemptions may apply. This subpart should be read together with the Privacy Act, which provides additional information about records maintained in agency systems of records, including those of the Department.

(2) This subpart contains the procedures that the Department follows when handling covered records maintained by the Department in a system of records, in accordance with the Judicial Redress Act of 2015, 5 U.S.C. 552a note (“Judicial Redress Act”). This subpart should be read together with the Privacy Act and the Judicial Redress Act, which provide additional information about covered records maintained in agency systems of records, including those of the Department.

(3) This subpart contains the procedures that the Department follows when collecting, using, maintaining, or disclosing Social Security account numbers, in accordance with the Privacy Act and the Social Security Number Fraud Prevention Act of 2017, 42 U.S.C. 405 note (“Social Security Number Fraud Prevention Act”). This subpart should be read together with the Privacy Act and the Social Security Number Fraud Prevention Act, which provide additional information about agencies’ maintenance of Social Security account numbers, including that of the Department.

(b) *Relationship to the Freedom of Information Act.* The Department also processes Privacy Act 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 benefits of both statutes.

(c) *Definitions.* In addition to the definitions found under 5 U.S.C. 552a(a), and section (2)(h) of the Judicial Redress Act, as used in this subpart:

*Component* means each separate bureau, office, board, division, commission, service, or administration of the Department.

*Privacy Act request for access* means a request made in accordance with 5 U.S.C. 552a(d)(1), and includes requests for a Privacy Act access appeal, in accordance with this subpart.

*Privacy Act request for amendment or correction* means a request made in accordance with 5 U.S.C. 552a(d)(2)-(4), and includes requests for a Privacy Act amendment or correction appeal, in accordance with this subpart.

*Privacy Act request for an accounting* means a request made in accordance with 5 U.S.C. 552a(c)(3).

*Requester* means an individual who makes a Privacy Act request for access, a Privacy Act request for amendment or correction, a Privacy Act request for an accounting, or, as provided by the Judicial Redress Act, a covered person who makes either a Privacy Act request for access or a Privacy Act request for amendment or correction to covered records.

*System of Records Notice* means the notice(s) published by the Department in the Federal Register upon the establishment or modification of a system of records describing the existence and character of the system of records. A System of Records Notice (“SORN”) may be composed of a single Federal Register notice addressing all of the

required elements that describe the current system of records, or it may be composed of multiple Federal Register notices that together address all of the required elements.

(d) *Authority to request records for a law enforcement purpose.* The head of a component or a United States Attorney, or either's designee, is authorized to make written requests under 5 U.S.C. 552a(b)(7), for records maintained by other agencies that are necessary to carry out an authorized law enforcement activity. The request must specify the particular portion desired and the law enforcement activity for which the record is sought.

(e) *Judicial Redress Act application.* (1) With respect to covered records, the Judicial Redress Act authorizes a covered person to bring a civil action against the Department and obtain civil remedies, in the same manner, to the same extent, and subject to the same limitations, including exemptions and exceptions, as an individual may bring a civil action and obtain civil remedies with respect to records under 5 U.S.C. 552a(g)(1)(A), (B).

(2) To the extent consistent with the Judicial Redress Act, when making a request for access, amendment, or correction to a covered record, a covered person must follow the procedures outlined in this subpart for making a Privacy Act request for access to a covered record, or a Privacy Act request for amendment or correction of a covered record. A covered person must exhaust the administrative remedies, as outlined in this subpart, before the covered person may bring a cause of action described in paragraph (e)(1) of this section.

(f) *Providing written consent to disclose records protected under the Privacy Act.* The Department may disclose any record contained in a system of records by any means

of communication to any person, or to another agency, pursuant to a written request by, or with the prior written consent of, the individual about whom the record pertains. An individual must verify the individual's identity in the same manner as required by § 16.41(d) when providing written consent to disclose a record protected under the Privacy Act and pertaining to the individual.

**§ 16.41 Privacy Act requests for access to records.**

(a) *General information.* (1) The Department has a decentralized system for responding to Privacy Act requests for access to records, with each component designating an office to process Privacy Act requests for access to records maintained by that component. A requester may make a Privacy Act request for access to records about the requester by writing directly to the component that maintains the records. All components have the capability to receive requests electronically either through email or a web portal. The request should be sent or delivered to the component's office at the address listed in appendix I to this part, or in accordance with the access procedures outlined in the corresponding SORN. The functions of each component are summarized in part 0 of this title and in the description of the Department and its components in the United States Government Manual, which is updated on a year-round basis and is available free of charge at <https://www.usgovernmentmanual.gov/>.

(2) If a requester cannot determine where within the Department to send the Privacy Act request for access to records, the requester may send it by mail to the FOIA/PA Mail Referral Unit, Justice Management Division, Department of Justice, 950 Pennsylvania Avenue NW., Washington, DC 20530-0001; by email to [MRUFOIA.Requests@usdoj.gov](mailto:MRUFOIA.Requests@usdoj.gov); or by fax to (202) 616-6695. The Mail Referral Unit

will forward the request to the component(s) it believes most likely to have the requested records. For the quickest possible handling, the requester should mark both the request letter and the envelope “Privacy Act Access Request.”

(b) *Description of records sought.* Requesters must describe the records sought in sufficient detail to enable Department personnel to locate the applicable system of records containing them with a reasonable amount of effort. To the extent possible, requesters should include specific information that may assist a component in identifying the requested records, such as the name or identifying number of each system of records in which the requester believes the records are maintained, or the date, title, name, author, recipient, case number, file designation, reference number, or subject matter of the record. The Department publishes SORNs in the Federal Register that describe the type and categories of records maintained in Department-wide and component-specific systems of records. Department SORNs may be found in published issues of the Federal Register and a list is available at <https://www.justice.gov/opcl/doj-systems-records>. Requesters may also request the record in a particular form or format.

(c) *Agreement to pay fees.* A Privacy Act request for access may specify the amount of fees that the requester is willing to pay in accordance with § 16.49. The component responsible for responding to the request shall confirm this agreement in an acknowledgement letter, in accordance with § 16.43.

(d) *Verification of identity.* (1) A requester must verify the requester’s identity when making a Privacy Act request for access. The requester must state the requester’s full name, current address, and date and place of birth. The requester must:

(i) Sign the request, and the signature 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; or

(ii) When available, use one of the Department's approved digital services, as indicated on the Department's Privacy Act Request webpage, to verify the identity of the requester through identity proofing and authentication processes.

(2) While no specific form is required, the requester may obtain forms for this purpose from the FOIA/PA Mail Referral Unit, Justice Management Division, Department of Justice, 950 Pennsylvania Avenue NW, Washington, DC 20530-0001, or obtain the form at <https://www.justice.gov/oip/doj-reference-guide-attachment-d-copies-forms>.

(3) To help identify and locate requested records, a requester may also include, at the requester's option, any additional identifying information which may be helpful in identifying and locating the requested records. Components shall establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of information provided by the requester, and to protect against any anticipated threats, in accordance with § 16.51.

(e) *Verification of guardianship.* (1) The parent of a minor, or the legal guardian of an individual who has been declared incompetent due to physical or mental incapacity or age by a court of competent jurisdiction, is permitted to act on behalf of the individual. In order for a parent of a minor or the legal guardian of an individual to make a Privacy Act request for access on behalf of the individual, the parent or legal guardian must establish:

(i) The identity of the individual who is the subject of the request, by stating the name, current address, date and place of birth, and, at the parent or legal guardian's option, any additional identifying information that may be helpful in identifying and locating the requested records;

(ii) The parent or legal guardian's own identity, as required in paragraph (d) of this section;

(iii) Proof of parentage or legal guardianship, which may be proven by providing a copy of the individual's birth certificate or by providing a court order establishing legal guardianship; and

(iv) That the parent or legal guardian is acting on behalf of that individual in making the request.

(2) Components shall establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of information provided by the parent or legal guardian, and to protect against any anticipated threats, in accordance with § 16.51.

**§ 16.42 Responsibility for responding to Privacy Act requests for access to records.**

(a) *In general.* Except as stated in paragraphs (c) through (f) of this section, the component that first receives a Privacy Act request for access 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 it maintained as of the date the component begins its search. If any other date is used, the component shall 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 Privacy Act request for access to records maintained by that component.

(c) *Re-routing of misdirected requests.* When a component's FOIA/Privacy Act office determines that a request was misdirected within the Department, the receiving component's FOIA/Privacy Act office shall route the request to the FOIA/Privacy Act office of the proper component(s).

(d) *Consultations, referrals, and coordination.* When a component receives a Privacy Act request for access to a record in its possession, it shall determine whether another component, or another agency of the Federal Government, is better able to determine whether the record is exempt from access under the Privacy Act. If the receiving component determines that it is best able to process the record in response to the request, then it shall do so. If the receiving component determines that it is not best able to process the record, then it shall follow the consultation, referral, and coordination procedures under § 16.4, subject to the requirements in this section. Components may make agreements with other components or agencies to eliminate the need for consultations or referrals for particular types of records.

(e) *Consultations, referrals, and coordination concerning law enforcement information.* When a component receives a Privacy Act request for access to a record in its possession containing information that relates to an investigation of a possible violation of law and that originated with another component or agency of the Federal Government, the receiving component shall either refer the responsibility for responding

to the request regarding that information to that other component or agency or shall consult with that other component or agency.

(f) *Consultations, referrals, and coordination concerning classified information.*

(1) When a component receives a Privacy Act request for access to a record containing information that has been classified or may be appropriate for classification by another component or agency under any applicable Executive order concerning the classification of records, the receiving component shall consult with or refer the responsibility for responding to the request regarding that information to the component or agency that classified the information, or that should consider the information for classification.

(2) When a component receives a Privacy Act request for access to a record containing information that has been derivatively classified, the receiving component shall consult with or refer the responsibility for responding to that portion of the request to the component or agency that classified the underlying information.

#### **§ 16.43 Responses to a Privacy Act requests for access to records.**

(a) *In general.* Components should, to the extent practicable, communicate with requesters who have access to the Internet using electronic means, such as through email or a web portal. A component shall honor a requester's preference for receiving a record in a particular form or format where it is readily reproducible by the component in the form or format requested.

(b) *Acknowledgement of requests.* The component responsible for responding to the request must acknowledge, in writing, receipt of a Privacy Act request for access. A component shall initially respond to the requester by acknowledging the Privacy Act request for access, assigning the request an individualized tracking number, and, if

applicable, confirming, in writing, the requester's agreement to pay fees in accordance with § 16.49.

(c) *Timing of responses to a Privacy Act request for access.* (1) Components ordinarily will respond to Privacy Act requests for access according to their order of receipt. The response time will commence on the date that the request is received by the proper component's office designated to receive requests, but in any event not later than ten (10) working days after the request is first received by any component's office designated by this subpart to receive requests.

(2) A component may designate multiple processing tracks that distinguish between simple and more complex Privacy Act requests for access, based on the estimated amount of work or time needed to process the request. Among the factors a component may consider are the number of pages involved in processing the request and the need for consultations or referrals. Components may advise requesters of the track into which their request falls and, when appropriate, may offer requesters an opportunity to narrow their request so that it can be placed in a different processing track.

(d) *Granting a Privacy Act request for access.* Once a component makes a determination to grant a Privacy Act request for access, in whole or in part, it shall notify the requester in writing. The component shall inform the requester in the notice of any fee charged under §16.49 and shall disclose records to the requester promptly on payment of any applicable fee.

(e) *Adverse determination to a Privacy Act request for access.* A component that makes an adverse determination to a Privacy Act request for access, in whole or in part, shall notify the requester of the adverse determination in writing. An adverse

determination to a Privacy Act request for access includes a determination by the component that: the request did not reasonably describe the record sought; the information requested is not a record subject to the Privacy Act; the requested record is not maintained in a system of records; the requested record is exempt, in whole or in part, from a Privacy Act request for access under applicable exemption(s); the requested record does not exist, cannot be located, or has been destroyed; the record is not readily reproducible in a comprehensible form; or there is a matter regarding disputed fees.

(f) *Content of adverse determination response.* An adverse determination to a Privacy Act request for access, in whole or in part, shall be signed by the head of the component, or the component head's designee, and shall include:

(1) The name and title or position of the person responsible for the adverse determination to the Privacy Act request for access;

(2) A brief statement of the reason(s) for the adverse determination to the Privacy Act request for access, including any Privacy Act exemption(s) applied by the component;

(3) An estimate of the volume of any records or information withheld, if applicable, such as the number of pages or some other reasonable form of estimation, although such an estimate is not required if the volume is otherwise indicated or if providing an estimate would harm an interest protected by an applicable exemption; and

(4) A statement that the adverse determination to the Privacy Act request for access may be appealed under § 16.45, and a description of the requirements set forth in § 16.45.

**§ 16.44 Classified information.**

In processing a Privacy Act request for access, a Privacy Act request for amendment or correction, or a Privacy Act request for accounting, in which information is classified under any applicable Executive order concerning the classification of records, to the extent the requester lacks the appropriate security clearance and fails otherwise to meet all requirements to access the classified record or information, the originating component shall review the information in the record to determine whether it should remain classified. Information determined to no longer require classification shall be de-classified and the record evaluated for an appropriate release to the requester, subject to any applicable exemptions or exceptions. On receipt of any appeal involving classified information, the official responsible for adjudicating the appeal shall take appropriate action to ensure compliance with part 17 of this title.

**§ 16.45 Privacy Act access appeals.**

(a) *Requirement for making a Privacy Act access appeal.* A requester may appeal an adverse determination to a Privacy Act request for access to the Office of Information Policy (“OIP”). The contact information for OIP is contained in the FOIA Reference Guide, which is available at [https://www.justice.gov/oip/04\\_3.html](https://www.justice.gov/oip/04_3.html). Appeals may also be submitted through the web portal accessible on OIP’s web site. Examples of an adverse determination to a Privacy Act request for access are provided in § 16.43. The requester must make the appeal in writing. To be considered timely, the requester must postmark, or in the case of electronic submissions, submit the request, within 90 calendar days after the date of the adverse determination. The appeal should indicate the assigned request number and clearly identify the component’s determination that is being appealed. To facilitate handling, the requester should mark both the appeal letter and envelope, or

include in the subject line of any electronic communication, “Privacy Act Access Appeal.”

(b) *Adjudication of Privacy Act access appeals.* (1) The Director of OIP, or a designee of the Director of OIP, shall act on behalf of the Attorney General on all Privacy Act access appeals under this section, unless the Attorney General directs otherwise.

(2) Should the Attorney General exercise the right to respond to a Privacy Act request for access, the Attorney General’s decision shall serve as the final action of the Department and will not be subject to a Privacy Act access appeal.

(3) A Privacy Act access appeal ordinarily will not be adjudicated if the request becomes a matter of litigation.

(c) *Responses to Privacy Act access appeals.* (1) OIP shall make its decision on an appeal in writing.

(2) A decision that upholds a component’s adverse determination to the Privacy Act request for access, in whole or in part, shall include a brief statement of the reason(s) for the affirmance, including any Privacy Act exemption applied, and shall provide the requester with notification of the statutory right to file a lawsuit.

(3) A decision that reverses or modifies, in whole or in part, a component’s adverse determination to the Privacy Act request for access shall include notice to the requester of the specific reversal or modification. The component(s) shall thereafter further process the request, in accordance with the appeal decision, and respond directly to the requester, as appropriate.

(d) *When a Privacy Act access appeal is required.* Before seeking review by a court of a component's refusal to grant a Privacy Act request for access, a requester generally must first submit a timely appeal in accordance with this section.

**§ 16.46 Privacy Act requests for amendment or correction.**

(a) *Requirements for making a Privacy Act request for amendment or correction.*

Unless the record is not subject to amendment or correction, as stated in paragraph (i) of this section, individuals may make a Privacy Act request for amendment or correction of a Department record about themselves. Requesters must write directly to the Department component that maintains the record. A Privacy Act request for amendment or correction shall identify each particular record in question, state the amendment or correction that the requester would like to make, and state why the requester believes the record is not accurate, relevant, timely, or complete. Requesters may submit any documentation that would be helpful in determining the accuracy, relevance, timeliness, or completeness of the record. If the requester believes that the same record is in more than one Department system of records, the requester should address the request to each component that the requester believes maintains the record. For the quickest possible handling, requesters should mark both their request letter and envelope "Privacy Act Amendment Request." Components and requesters must otherwise follow the procedures and responsibilities set forth in §§ 16.41 and 16.42.

(b) *Timing of responses to a Privacy Act request for amendment or correction.* (1)

Components responsible for responding to a Privacy Act request for amendment or correction must acknowledge, in writing, receipt of the request no later than ten (10) working days after receipt.

(2) Components must promptly respond to a Privacy Act request for amendment or correction. Components ordinarily will respond to Privacy Act requests for amendment or correction according to their order of receipt. The response time will commence on the date that the request is received by the proper component's office designated to receive requests, but in any event no later than ten (10) working days after the request is first received by any component's office designated by this subpart to receive requests.

(3) A component may designate multiple processing tracks that distinguish between simple and more complex Privacy Act requests for amendment or correction, based on the estimated amount of work or time needed to process the request. Among the factors a component may consider are the number of pages involved in processing the request and the need for consultations or referrals. Components may advise requesters of the track into which their request falls and, when appropriate, may offer requesters an opportunity to narrow their request so that it can be placed in a different processing track.

(c) *Granting a Privacy Act request for amendment or correction.* If a component grants a Privacy Act request for amendment or correction, in whole or in part, it shall notify the requester in writing. The component shall describe the amendment or correction made and shall advise the requester of the requester's right to obtain a copy of the corrected or amended record, in accordance with the Privacy Act right of access procedures described in §§ 16.41 through 16.45.

(d) *Adverse determination to a Privacy Act request for amendment or correction.* A component that makes an adverse determination to a Privacy Act request for amendment or correction, in whole or in part, shall notify the requester of the

determination in writing. An adverse determination to a Privacy Act request for amendment or correction includes a decision by the component that: the information at issue is not a record as defined by the Privacy Act; the requested record is not subject to amendment or correction as stated in paragraph (i) of this section; the request does not reasonably describe the records sought or the amendment or correction to that record; the record at issue does not exist, cannot be located, has been destroyed, or otherwise cannot be amended or corrected; or the record is maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness in any determination about the individual about whom the record pertains.

(e) *Content of adverse determination response.* An adverse determination to a Privacy Act request for amendment or correction, in whole or in part, shall be signed by the head of the component, or the component head's designee, and shall include:

(1) The name and title or position of the person responsible for the adverse determination to the Privacy Act request for amendment or correction;

(2) A brief statement of the reason(s) for the adverse determination to the Privacy Act request for amendment or correction, including any Privacy Act exemption(s) applied by the component; and

(3) A statement that the adverse determination to the Privacy Act request for amendment or correction may be appealed under paragraph (f) of this section and a description of the requirements set forth in paragraph (f).

(f) *Privacy Act amendment appeals.* (1) A requester may appeal an adverse determination to a Privacy Act request for amendment or correction, in whole or in part, to the Office of Privacy and Civil Liberties ("OPCL"). The contact information for OPCL

is available at <https://www.justice.gov/privacy>. The requester must make the appeal in writing. To be considered timely, the requester must postmark the appeal request, or in the case of electronic submissions, submit the appeal request, within 90 calendar days after the date of the component's refusal to grant a Privacy Act request for amendment or correction. The appeal should indicate the assigned request number and clearly identify the component's determination that is being appealed. To facilitate handling, the requester should mark both the appeal letter and envelope, or include in the subject line of the electronic transmission, "Privacy Act Amendment Appeal."

(2) The Chief Privacy and Civil Liberties Officer ("CPCLO"), or a designee of the CPCLO, will act on behalf of the Attorney General on all Privacy Act amendment appeals under this section, unless otherwise directed by the Attorney General.

(3) A Privacy Act amendment appeal ordinarily will not be adjudicated if the request becomes a matter of litigation.

(4) A decision on a Privacy Act amendment appeal must be made in writing. A decision that upholds a component's adverse determination to a Privacy Act request for amendment or correction, in whole or in part, shall include a brief statement of the reason(s) for the affirmance, including any Privacy Act exemption applied, whether the requester has a right to file a Statement of Disagreement, as described in paragraph (g) of this section, and the requester's statutory right to file a lawsuit. A decision that reverses or modifies a component's adverse determination to a Privacy Act request for amendment or correction, in whole or in part, shall notify the requester of the specific reversal or modification. The component shall thereafter further process the request, in accordance with the appeal decision, and respond directly to the requester, as appropriate.

(g) *Statement of Disagreement.* If a request is subject to a Privacy Act request for amendment or correction, but the component's adverse determination to a Privacy Act request for amendment or correction is upheld, in whole or in part, the requester has the right to file a Statement of Disagreement that states the requester's reason(s) for disagreeing with the Department's refusal to grant the requester's Privacy Act 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. A Statement of Disagreement must be sent to the component involved, which shall place it in the system of records in which the disputed record is maintained so that the Statement of Disagreement supplements the disputed record. The component shall 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.

(h) *Notification of amendment, correction, or Statement of Disagreement.* Within thirty (30) working days of the amendment or correction of a record, the component that maintains the record shall notify all persons, organizations, or agencies to which it previously disclosed the record, if an accounting of that disclosure was made, that the record has been amended or corrected. If an individual has filed a Statement of Disagreement, the component shall append a copy of it to the disputed record whenever the record is disclosed. The component may also append a concise statement of its reason(s) for denying the Privacy Act request for amendment or correction of the record.

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

- (1) Copies of court records;

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

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

(4) Presentence reports, and other records pertaining directly to such reports originating with the courts;

(5) Records in a system of records that have been exempted from amendment and correction, pursuant to 5 U.S.C. 552a(j) or (k), through the applicable regulations in this subpart; and

(6) Records not maintained in a system of records.

**§ 16.47 Privacy Act requests for an accounting of record disclosures.**

(a) *Requirements for making a Privacy Act request for accounting of record disclosures.* Except where accountings of disclosures are not required to be kept as stated in paragraph (c) of this section, individuals may make a Privacy Act request for an accounting of record disclosures about themselves that have been made by the Department to another person, organization, or agency. 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. If the requester believes that the same record is in more than one system of records, the requester should address their request to each component that the requester believes maintains the record. For the quickest possible handling, requesters should mark both their request letters and envelopes “Privacy Act Accounting Request.” Requests must otherwise follow the procedures in § 16.41.

(b) *Processing Privacy Act requests for an accounting of record disclosures.*

Unless otherwise specified in this section, components shall process Privacy Act requests for accountings of record disclosures following the procedures in §§ 16.42 and 16.43.

(c) *Where accountings of record disclosures are not required.* Components are not required to provide Privacy Act accountings of record disclosures to a requester in cases in which they relate to:

(1) Disclosures of information not subject to the Privacy Act;

(2) Disclosures of records not maintained in a system of records;

(3) Disclosures of records maintained in a system of records for which accountings are not required to be kept, including disclosures to those officers and employees of the Department who have a need for the record in the performance of their duties, 5 U.S.C. 552a(b)(1), or disclosures that are required under the FOIA, 5 U.S.C 552a(b)(2);

(4) 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

(5) Disclosures made from systems of records that have been exempted from the accounting of record disclosure requirements pursuant to the Privacy Act, 5 U.S.C. 552a(j) or (k), through the applicable regulations in this subpart.

(d) *Appeals.* A requester may appeal a component's refusal to grant a Privacy Act request for an accounting of record disclosures in the same manner, and under the same procedures, as a Privacy Act access appeal, as set forth in §16.45.

#### **§ 16.48 Preservation of records.**

Each component shall 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 by the National Archives and Records Administration's General Records Schedule 4.2. Records shall not be disposed of while they are the subject of a pending request, appeal, or lawsuit under the Privacy Act.

**§ 16.49 Fees.**

Components shall charge fees for duplication of records under the Privacy Act in the same way in which they charge duplication fees for responding to FOIA requests under §16.10. No search or review fee may be charged for any record unless the record has been exempted from access pursuant to exemptions enumerated in the Privacy Act, 5 U.S.C. 552a(j)(2) or (k)(2).

**§ 16.50 Notice of compulsory legal process and emergency disclosures.**

(a) *Legal process disclosures.* Components shall make reasonable efforts to provide notice to an individual whose record is disclosed under compulsory legal process, such as an order by a court of competent jurisdiction, and such process becomes a matter of public record. Notice shall be given within a reasonable time after the component's receipt of process, except that in a case in which such process is not a matter of public record, the notice shall be given within a reasonable time only after such process becomes public. Where an individual, or the individual's legal counsel, has not otherwise received notice of the disclosure in the litigation process, notice shall be mailed to the individual's last known address and shall contain a copy of such process and a

description of the information disclosed. Notice shall not be required if disclosure is made from a system of records that has been exempted from the notice requirement.

(b) *Emergency disclosures.* Upon disclosing a record pertaining to an individual made under compelling circumstances affecting health or safety, the component shall notify that individual of the disclosure. This notice shall be mailed to the individual's last known address and shall 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.

**§ 16.51 Security of systems of records.**

(a) Each component shall establish and maintain administrative, technical, and physical controls consistent with applicable Department and Government-wide laws, regulations, policies, and standards, to ensure the security and confidentiality of records, and to protect against reasonably anticipated threats or hazards to their security or integrity, including against any reasonably anticipated unauthorized access, use, or disclosure, which could result in substantial harm, embarrassment, inconvenience, or unfairness to individuals about whom information is maintained. The stringency of these controls shall correspond to the sensitivity of the records that the controls protect. At a minimum, each component shall maintain administrative, technical, or physical controls to ensure that:

(1) Records are protected from unauthorized access, including unauthorized public access;

(2) The physical area in which records are maintained is supervised or appropriately secured to prevent unauthorized persons from having access to them;

(3) Records are protected from damage, loss, or unauthorized alteration or destruction; and

(4) Records are not disclosed to unauthorized persons or to authorized persons for unauthorized purposes in either oral or written form.

(b) Each component shall establish procedures that restrict access to records to only those individuals within the Department who must have access to those records in order to perform their duties and that prevent inadvertent disclosure of records.

(c) The CPCLO, or a designee of the CPCLO, may impose additional administrative, technical, or physical controls to protect records in consultation with the Chief Information Officer and the Director of the Office of Records Management Policy.

#### **§ 16.52 Contracts for the operation of record systems.**

(a) Any approved contract for the operation of a system of records shall contain the standard contract terms and conditions in accordance with the Federal Acquisition Regulations in 48 CFR chapter 28 and may also contain additional privacy-related terms and conditions to ensure compliance with the requirements of the Privacy Act for that system of records. The contracting component will be responsible for ensuring that the contractor complies with these contract requirements.

(b) The CPCLO, a designee of the CPCLO, or contracting components may impose additional contract requirements to further protect records.

#### **§ 16.53 Use and collection of Social Security account numbers.**

(a) *Purpose and scope.* This section contains the rules that the Department of Justice follows in handling Social Security account numbers in accordance with section 7 of the Privacy Act, and with the Social Security Fraud Prevention Act.

(b) *Definitions.* For the purposes of this section:

*Mail* means any physical package sent to entities or individuals outside the Department through the United States Postal Service or any other express mail carrier; and

*Necessary* includes only those circumstances in which a component would be unable to comply, in whole or in part, with a legal, regulatory, or policy requirement if prohibited from mailing the full Social Security account number. Including the full Social Security account number of an individual on a document sent by mail is not “necessary” if a legal, regulatory, or policy requirement could be satisfied by either partially redacting the Social Security account number in accordance with paragraph (d)(3) of this section, or entirely removing the Social Security account number.

(c) *Denial of rights, benefits, or privileges.* Components are prohibited from denying any right, benefit, or privilege provided by law to an individual because of such individual’s refusal to disclose the individual’s Social Security account number. This paragraph (c) shall not apply with respect to:

(1) Any disclosure that is required by Federal statute; or

(2) The disclosure of a Social Security account number to any Federal, State, or local agency maintaining a system of records in existence and operating before January 1, 1975, if such disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual.

(d) *Restriction of Social Security account numbers on documents sent by mail.* (1) A component shall not include the full Social Security account number of an individual on any document sent by mail, unless the inclusion of the Social Security account number

on the document is necessary. Unless the Attorney General directs otherwise, the CPCLCLO is authorized to assist components in implementing this paragraph (d), including determining whether inclusion of the Social Security account number on a document sent by mail is necessary.

(2) If the use of the full Social Security account number on a document sent by mail is necessary, the component sending the document shall implement appropriate administrative, technical, and physical safeguards to ensure a reasonable level of security against unauthorized access to, and use, disclosure, disruption, modification, or destruction of, the documents sent by mail.

(3) Where feasible, components should partially redact the Social Security account number on any document sent by mail by including no more than the last four digits of the Social Security account number. Components should prioritize technical methods to redact Social Security account numbers.

(4) Components are prohibited from placing a Social Security account number, whether full or partially redacted, on the outside of any mail.

(e) *Employee awareness.* Each component shall ensure that employees authorized to collect Social Security account numbers are made aware of the following:

(1) The requirements of paragraphs (c) and (d) of this section;

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

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

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

(iii) The uses that will be made of the Social Security account numbers; and

(3) That the Department may have other regulations or policies regulating the use, maintenance, or disclosure of Social Security account numbers by which employees must abide.

**§ 16.54 Employee standards of conduct.**

Each component shall inform its employees and any contractors involved in developing or maintaining a system of records of the provisions of the Privacy Act, including the Privacy Act's civil liability and criminal penalty provisions. Unless otherwise permitted by law, employees and contractors of the Department shall:

(a) Collect from individuals only the information that is relevant and necessary to discharge the responsibilities of the Department;

(b) Collect information about an individual directly from that individual whenever practicable;

(c) Inform each individual asked to supply information for a record pertaining to that individual 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 the individual's First Amendment rights, unless maintaining the record 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 Privacy 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 loss or the unauthorized or inadvertent disclosure of a record to anyone;

(j) Notify the appropriate Department official of any record that contains information that the Privacy Act does not permit the Department to maintain; and

(k) Read, acknowledge, and agree to abide by the Department of Justice rules of behavior for accessing, collecting, using, and maintaining Department information.

**§ 16.55 Other rights and services.**

Nothing in this subpart shall 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, the Social Security Fraud Reduction Act, or the Judicial Redress Act.

3. Amend appendix I to part 16 by revising the first two paragraphs to read as follows:

**Appendix I to Part 16--Components of the Department of Justice**

Please consult Attachment B of the Department of Justice FOIA Reference Guide for the contact information and a detailed description of the types of records maintained by each Department component. The FOIA Reference Guide is available at <https://www.justice.gov/oip/department-justice-freedom-information-act-reference-guide> or upon request to the Office of Information Policy (OIP).

The Department component offices, and any component-specific requirements, for making a FOIA or Privacy Act request are listed in this appendix. The Certification of Identity form, available at <https://www.justice.gov/oip/doj-reference-guide-attachment-d-copies-forms>, may be used by individuals who are making requests for records pertaining to themselves. For each of the six components marked with an asterisk, FOIA and Privacy Act requests for access must be sent to OIP, which handles initial requests for those six components.

\* \* \* \* \*

Dated: January 2, 2024.

**Merrick B. Garland,**

*Attorney General.*

[FR Doc. 2024-00282 Filed: 1/9/2024 8:45 am; Publication Date: 1/10/2024]