

## § 3.9

### § 3.9 Responding to a rulemaking petition.

(a) *Public procedure.* DHS may, in its discretion, seek broader public comment on a rulemaking petition prior to its disposition under this section.

(b) *Disposition.* DHS may respond to the petition by letter or by FEDERAL REGISTER publication. DHS may grant or deny the petition, in whole or in part.

(c) *Grounds for denial.* DHS may deny the petition for any reason consistent with law, including, but not limited to, the following reasons: The petition has no merit, the petition is contrary to pertinent statutory authority, the petition is not supported by the relevant information or data, or the petition cannot be addressed because of other priorities or resource constraints.

(d) *Summary disposition.* DHS may, by written letter, deny or summarily dismiss without prejudice any petition that is moot, premature, repetitive, or frivolous, or that plainly does not warrant further consideration.

## PART 4 [RESERVED]

## PART 5—DISCLOSURE OF RECORDS AND INFORMATION

### Subpart A—Procedures for Disclosure of Records Under the Freedom of Information Act

#### Sec.

- 5.1 General provisions.
- 5.2 Proactive disclosures of DHS records.
- 5.3 Requirements for making requests.
- 5.4 Responsibility for responding to requests.
- 5.5 Timing of responses to requests.
- 5.6 Responses to requests.
- 5.7 Confidential commercial information.
- 5.8 Administrative appeals.
- 5.9 Preservation of records.
- 5.10 FOIA requests for information contained in a Privacy Act system of records.
- 5.11 Fees.
- 5.12 Confidential commercial information; CBP procedures.
- 5.13 Other rights and services.

#### APPENDIX I TO SUBPART A OF PART 5—FOIA CONTACT INFORMATION

### Subpart B—Privacy Act

- 5.20 General provisions.

## 6 CFR Ch. I (1–1–20 Edition)

- 5.21 Requests for access to records.
- 5.22 Responsibility for responding to requests for access to records.
- 5.23 Responses to requests for access to records.
- 5.24 Classified information.
- 5.25 Appeals.
- 5.26 Requests for amendment or correction of records.
- 5.27 Requests for an accounting of record disclosures.
- 5.28 Preservation of records.
- 5.29 Fees.
- 5.30 Notice of court-ordered and emergency disclosures.
- 5.31 Security of systems of records.
- 5.32 Contracts for the operation of record systems.
- 5.33 Use and collection of social security numbers.
- 5.34 Standards of conduct for administration of the Privacy Act.
- 5.35 Sanctions and penalties.
- 5.36 Other rights and services.

### Subpart C—Disclosure of Information in Litigation

- 5.41 Purpose and scope; definitions.
- 5.42 Service of summonses and complaints.
- 5.43 Service of subpoenas, court orders, and other demands or requests for official information or action.
- 5.44 Testimony and production of documents prohibited unless approved by appropriate Department officials.
- 5.45 Procedure when testimony or production of documents is sought; general.
- 5.46 Procedure when response to demand is required prior to receiving instructions.
- 5.47 Procedure in the event of an adverse ruling.
- 5.48 Considerations in determining whether the Department will comply with a demand or request.
- 5.49 Prohibition on providing expert or opinion testimony.

#### APPENDIX A TO PART 5—FOIA/PRIVACY ACT OFFICES OF THE DEPARTMENT OF HOMELAND SECURITY

#### APPENDIX B TO PART 5 [RESERVED]

#### APPENDIX C TO PART 5—DHS SYSTEMS OF RECORDS EXEMPT FROM THE PRIVACY ACT

AUTHORITY: 6 U.S.C. 101 *et seq.*; Pub. L. 107–296, 116 Stat. 2135; 5 U.S.C. 301.

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

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

SOURCE: 68 FR 4056, Jan. 27, 2003, unless otherwise noted.

### Subpart A—Procedures for Disclosure of Records Under the Freedom of Information Act

SOURCE: 81 FR 83632, Nov. 22, 2016, unless otherwise noted.

#### § 5.1 General provisions.

(a)(1) This subpart contains the rules that the Department of Homeland Security follows in processing requests for records under the Freedom of Information Act (FOIA), 5 U.S.C. 552 as amended.

(2) The rules in this subpart should be read in conjunction with the text of the FOIA and the Uniform Freedom of Information Fee Schedule and Guidelines published by the Office of Management and Budget at 52 FR 10012 (March 27, 1987) (hereinafter “OMB Guidelines”). Additionally, DHS has additional policies and procedures relevant to the FOIA process. These resources are available at <http://www.dhs.gov/freedom-information-act-foia>. Requests made by individuals for records about themselves under the Privacy Act of 1974, 5 U.S.C. 552a, are processed under subpart B of part 5 as well as under this subpart.

(b) As referenced in this subpart, component means the FOIA office of each separate organizational entity within DHS that reports directly to the Office of the Secretary.

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

(d) *Unofficial release of DHS information.* The disclosure of exempt records, without authorization by the appropriate DHS official, is not an official release of information; accordingly, it is not a FOIA release. Such a release does not waive the authority of the Department of Homeland Security to assert FOIA exemptions to withhold the same records in response to a FOIA request. In addition, while the authority may exist to disclose records to individuals in their official capacity, the provisions of this part apply if the same individual seeks the records in a private or personal capacity.

#### § 5.2 Proactive disclosure of DHS records.

Records that are required by the FOIA to be made available for public inspection in an electronic format are accessible on DHS’s Web site, <http://www.dhs.gov/freedom-information-act-foia-and-privacy-act>. Each component is responsible for determining which of its records are required to be made publicly available, as well as identifying additional records of interest to the public that are appropriate for public disclosure, and for posting and indexing such records. Each component shall ensure that posted records and indices are updated on an ongoing basis. Each component has a FOIA Public Liaison who can assist individuals in locating records particular to a component. A list of DHS’s FOIA Public Liaisons is available at <http://www.dhs.gov/foia-contact-information> and in appendix I to this subpart. Requesters who do not have access to the internet may contact the Public Liaison for the component from which they seek records for assistance with publicly available records.

#### § 5.3 Requirements for making requests.

(a) *General information.* (1) DHS has a decentralized system for responding to FOIA requests, with each component designating a FOIA office to process records from that component. All components have the capability to receive requests electronically, either through email or a web portal. To make a request for DHS records, a requester should write directly to the FOIA office of the component that maintains the records being sought. A request will receive the quickest possible response if it is addressed to the FOIA office of the component that maintains the records sought. DHS’s FOIA Reference Guide contains or 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 I of this subpart. These references can all be used by requesters to

## §5.4

## 6 CFR Ch. I (1–1–20 Edition)

determine where to send their requests within DHS.

(2) A requester may also send his or her request to the Privacy Office, U.S. Department of Homeland Security, 245 Murray Lane SW STOP-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.

(3) A requester who is making a request for records about him or herself must comply with the verification of identity provision set forth in subpart B of this part.

(4) Where a request for records pertains to a third party, a requester may receive greater access by submitting either a notarized authorization signed by that individual, in compliance with the verification of identity provision set forth in subpart B of this part, or a declaration made in compliance with the requirements set forth in 28 U.S.C. 1746 by that individual, authorizing disclosure of the records to the requester, or by submitting proof that the 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 requester to supply additional information if necessary in order to verify that a particular individual has consented to disclosure.

(b) *Description of records sought.* Requesters must describe the records sought in sufficient detail to enable DHS personnel to locate them with a reasonable amount of effort. A reasonable description contains sufficient information to permit an organized, non-random search for the record based on the component's filing arrangements and existing retrieval systems. To the extent possible, requesters should include specific information that may assist a component in identifying the requested records, such as the date, title or name, author, recipient, subject matter of the record, case number, file designation, or reference number. Requesters should refer to appendix I of this subpart for additional component-specific requirements. In general, requesters should include as much detail

as possible about the specific records or the types of records that they are seeking. Before submitting their requests, requesters may contact the component's FOIA Officer or FOIA public liaison to discuss the records they are seeking and to receive assistance in describing the records. If after receiving a request, a component determines that it does not reasonably describe the records sought, the component should inform the requester what additional information is needed or why the request is otherwise insufficient. Requesters who are attempting to reformulate or modify such a request may discuss their request with the component's designated FOIA Officer, its FOIA Public Liaison, or a representative of the DHS Privacy Office, each of whom is available to assist the requester in reasonably describing the records sought.

(c) 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. In order 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 or received by electronic mail by 11:59:59 p.m. ET on the 30th working day. If the requester does not respond to a request for additional information within thirty (30) working days, 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.

### §5.4 Responsibility for responding to requests.

(a) *In general.* Except in the instances described in paragraphs (c) and (d) of this section, the component that first

receives a request for a record and maintains 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 records in its possession as of the date that it begins its search. If any other date is used, the component shall inform the requester of that date. A record that is excluded from the requirements of the FOIA pursuant to 5 U.S.C. 552(c), shall not be considered responsive to a request.

(b) *Authority to grant or deny requests.* The head of a component, or designee, is authorized to grant or to deny any requests for records that are maintained by that component.

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

(d) *Consultations, coordination and referrals.* When a component determines that it maintains responsive records that either originated with another component or agency, or which contains information provided by, or of substantial interest to, another component or agency, then it shall proceed in accordance with either paragraph (d)(1), (2), or (3) of this section, as appropriate:

(1) The component may respond to the request, after consulting with the component or the agency that originated or has a substantial interest in the records involved.

(2) The component may respond to the request after coordinating with the other components or agencies that originated the record. This may include situations where the standard referral procedure is not appropriate where disclosure of the identity of the component or agency to which the referral would be made could harm an interest protected by an applicable exemption, such as the exemptions that protect personal privacy or national security interests. For example, if a non-law enforcement component responding to a request for records on a living third party locates records within its files originating with a law enforce-

ment agency, and if the existence of that law enforcement interest in the third party was not publicly known, then to disclose that law enforcement interest could cause an unwarranted invasion of the personal privacy of the third party. Similarly, if a component locates material within its files originating with an Intelligence Community agency, and the involvement of that agency in the matter is classified and not publicly acknowledged, then to disclose or give attribution to the involvement of that Intelligence Community agency could cause national security harms. In such instances, in order to avoid harm to an interest protected by an applicable exemption, the component that received the request should coordinate with the originating component or agency to seek its views on the disclosability of the record. The release determination for the record that is the subject of the coordination should then be conveyed to the requester by the component that originally received the request.

(3) The component may refer the responsibility for responding to the request or portion of the request to the component or agency best able to determine whether to disclose the relevant records, or to the agency that created or initially acquired the record as long as that agency is subject to the FOIA. Ordinarily, the component or agency that created or initially acquired the record will be presumed to be best able to make the disclosure determination. The referring component shall document the referral and maintain a copy of the records that it refers.

(e) *Classified information.* On receipt of any request involving classified information, the component shall determine whether information is currently and properly classified and take appropriate action to ensure compliance with 6 CFR part 7. Whenever a request involves 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 refer the responsibility for responding to the request regarding that information to

## §5.5

## 6 CFR Ch. I (1–1–20 Edition)

the component or agency that classified the information, or should consider the information for classification. Whenever a component's record contains information classified by another component or agency, the component shall coordinate with or refer the responsibility for responding to that portion of the request to the component or agency that classified the underlying information.

(f) *Notice of referral.* Whenever a component refers any part of the responsibility for responding to a request to another component or agency, it will notify the requester of the referral and inform the requester of the name of each component or agency to which the records were referred, unless disclosure of the identity of the component or agency would harm an interest protected by an applicable exemption, in which case the component should coordinate with the other component or agency, rather than refer the records.

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

(h) *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 particular types of records.

(1) *Electronic records and searches—(1) Significant interference.* The FOIA allows components to not conduct a search for responsive documents if the search would cause significant interference with the operation of the component's automated information system.

(2) *Business as usual approach.* A "business as usual" approach exists when the component has the capability to process a FOIA request for electronic records without a significant expenditure of monetary or personnel resources. Components are not required to conduct a search that does not meet this business as usual criterion.

(i) Creating computer programs or purchasing additional hardware to extract email that has been archived for emergency retrieval usually are not

considered business as usual if extensive monetary or personnel resources are needed to complete the project.

(ii) Creating a computer program that produces specific requested fields or records contained within a well-defined database structure usually is considered business as usual. The time to create this program is considered as programmer or operator search time for fee assessment purposes and the FOIA requester may be assessed fees in accordance with §5.11(c)(1)(iii). However, creating a computer program to merge files with disparate data formats and extract specific elements from the resultant file is not considered business as usual, but a special service, for which additional fees may be imposed as specified in §5.11. Components are not required to perform special services and creation of a computer program for a fee is up to the discretion of the component and is dependent on component resources and expertise.

(3) *Data links.* Components are not required to expend DHS funds to establish data links that provide real time or near-real-time data to a FOIA requester.

### §5.5 Timing of responses to requests.

(a) *In general.* Components ordinarily will respond to requests according to their order of receipt. Appendix I to this subpart contains the list of components that are designated to accept requests. In instances involving misdirected requests that are re-routed pursuant to §5.4(c), the response time will commence on the date that the request is received by the proper component, but in any event not later than ten working days after the request is first received by any DHS component designated in appendix I of this subpart.

(b) *Multitrack processing.* All components must designate a specific track for requests that are granted expedited processing, in accordance with the standards set forth in paragraph (e) of this section. A component may also designate additional processing tracks that distinguish between simple and more complex requests 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 or the need for consultations or referrals. Components shall advise requesters of the track into which their request falls, and when appropriate, shall offer requesters an opportunity to narrow their request so that the request can be placed in a different processing track.

(c) *Unusual circumstances.* Whenever the statutory time limits for processing a request cannot be met because of “unusual circumstances,” as defined in the FOIA, and the component extends the time limits on that basis, the component shall, before expiration of the twenty-day period to respond, notify the requester in writing of the unusual circumstances involved and of the date by which processing of the request can be expected to be completed. Where the extension exceeds ten working days, the component shall, as described by the FOIA, provide the requester with an opportunity to modify the request or agree to an alternative time period for processing. The component shall make available its designated FOIA Officer and its FOIA Public Liaison for this purpose. The component shall also alert requesters to the availability of the Office of Government Information Services (OGIS) to provide dispute resolution services.

(d) *Aggregating requests.* For the purposes of satisfying unusual circumstances under the FOIA, components may aggregate requests in cases where it reasonably appears that multiple requests, submitted either by a requester or by a group of requesters acting in concert, constitute a single request that would otherwise involve unusual circumstances. Components will not aggregate multiple requests that involve unrelated matters.

(e) *Expedited processing.* (1) Requests and appeals will be processed on an expedited basis whenever the component determines that they involve:

(i) Circumstances in which the lack of expedited processing could reasonably be expected to pose an imminent threat to the life or physical safety of an individual;

(ii) An urgency to inform the public about an actual or alleged federal government activity, if made by a person

who is primarily engaged in disseminating information;

(iii) The loss of substantial due process rights; or

(iv) A matter of widespread and exceptional media interest in which there exist possible questions about the government’s integrity which affect public confidence.

(2) A request for expedited processing may be made at any time. Requests based on paragraphs (e)(1)(i), (ii), and (iii) of this section must be submitted to the component that maintains the records requested. When making a request for expedited processing of an administrative appeal, the request should be submitted to the DHS Office of General Counsel or the component Appeals Officer. Address information is available at the DHS Web site, <http://www.dhs.gov/freedom-information-act-foia>, or by contacting the component FOIA officers via the information listed in appendix I. Requests for expedited processing that are based on paragraph (e)(1)(iv) of this section must be submitted to the Senior Director of FOIA Operations, the Privacy Office, U.S. Department of Homeland Security, 245 Murray Lane SW STOP-0655, Washington, DC 20598-0655. A component that receives a misdirected request for expedited processing under the standard set forth in paragraph (e)(1)(iv) of this section shall forward it immediately to the DHS Senior Director of FOIA Operations, the Privacy Office, for determination. The time period for making the determination on the request for expedited processing under paragraph (e)(1)(iv) of this section shall commence on the date that the Privacy Office receives the request, provided that it is routed within ten working days, but in no event shall the time period for making a determination on the request commence any later than the eleventh working day after the request is received by any component designated in appendix I of this subpart.

(3) A requester who seeks expedited processing must submit a statement, certified to be true and correct, explaining in detail the basis for making the request for expedited processing. For example, under paragraph (e)(1)(ii) of this section, a requester who is not a full-time member of the news media

## §5.6

## 6 CFR Ch. I (1–1–20 Edition)

must establish that he or she is a person who primarily engages in information dissemination, though it need not be his or her sole occupation. Such a requester also must establish a particular urgency to inform the public about the government activity involved in the request—one that extends beyond the public's right to know about government activity generally. The existence of numerous articles published on a given subject can be helpful to establishing the requirement that there be an "urgency to inform" the public on the topic. As a matter of administrative discretion, a component may waive the formal certification requirement.

(4) A component shall notify the requester within ten calendar days of the receipt of a request for expedited processing of its decision whether to grant or deny expedited processing. If expedited processing is granted, the request shall be given priority, placed in the processing track for expedited requests, and shall be processed as soon as practicable. If a request for expedited processing is denied, any appeal of that decision shall be acted on expeditiously.

### §5.6 Responses to requests.

(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) *Acknowledgments of requests.* A component shall acknowledge the request and assign it an individualized tracking number if it will take longer than ten working days to process. Components shall include in the acknowledgment a brief description of the records sought to allow requesters to more easily keep track of their requests.

(c) *Grants of requests.* Ordinarily, a component shall 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. Once a component makes a determination to grant a request in full or in part, it shall notify the requester in writing. The component also shall inform the requester of any fees charged

under §5.11 and shall disclose the requested records to the requester promptly upon payment of any applicable fees. The component shall inform the requester of the availability of its FOIA Public Liaison to offer assistance.

(d) *Adverse determinations of requests.* A component making an adverse determination denying a request in any respect shall 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 request does not reasonably describe the records sought; the information requested is not a record subject to the FOIA; the requested record does not exist, cannot be located, or has been destroyed; or the requested record is not readily reproducible in the form or format sought by the requester. Adverse determinations also include denials involving fees, including requester categories or fee waiver matters, or denials of requests for expedited processing.

(e) *Content of denial.* The denial shall be signed by the head of the component, or designee, and shall include:

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

(2) A brief statement of the reasons for the denial, including any FOIA exemption applied by the component in denying the request;

(3) An estimate of the volume of any records or information withheld, for example, by providing the number of pages or some other reasonable form of estimation. This estimation is not required if the volume is otherwise indicated by deletions marked on records that are disclosed in part, or if providing an estimate would harm an interest protected by an applicable exemption; and

(4) A statement that the denial may be appealed under §5.8(a), and a description of the requirements set forth therein.

(5) A statement notifying the requester of the assistance available from the agency's FOIA Public Liaison and the dispute resolution services offered by OGIS.

(f) *Markings on released documents.* Markings on released documents must

be clearly visible to the requester. Records disclosed in part shall be marked to show the amount of information deleted and the exemption under which the deletion was made unless doing so would harm an interest protected by an applicable exemption. The location of the information deleted also shall be indicated on the record, if technically feasible.

(g) *Use of record exclusions.* (1) In the event that a component identifies records that may be subject to exclusion from the requirements of the FOIA pursuant to 5 U.S.C. 552(c), the head of the FOIA office of that component must confer with Department of Justice's Office of Information Policy (OIP) to obtain approval to apply the exclusion.

(2) Any component invoking an exclusion shall maintain an administrative record of the process of invocation and approval of the exclusion by OIP.

#### § 5.7 Confidential commercial information.

(a) *Definitions*—(1) *Confidential commercial information* means commercial or financial information obtained by DHS from a submitter that may be protected from disclosure under Exemption 4 of the FOIA.

(2) *Submitter* means any person or entity from whom DHS obtains confidential commercial information, directly or indirectly.

(b) *Designation of confidential commercial information.* A submitter of confidential commercial information must use good faith efforts to designate by appropriate markings, either at the time of submission or within a reasonable time thereafter, any portion of its submission that it considers to be protected from disclosure under Exemption 4. These designations will expire ten years after the date of the submission unless the submitter requests and provides justification for a longer designation period.

(c) *When notice to submitters is required.* (1) A component shall promptly provide written notice to a submitter whenever records containing such information are requested under the FOIA if, after reviewing the request, the responsive records, and any appeal by the requester, the component deter-

mines that it may be required to disclose the records, provided:

(i) The requested information has been designated in good faith by the submitter as information considered protected from disclosure under Exemption 4; or

(ii) The component has a reason to believe that the requested information may be protected from disclosure under Exemption 4.

(2) The notice shall either describe the commercial information requested or include a copy of the requested records or portions of records containing the information. In cases involving a voluminous number of submitters, notice may be made by posting or publishing the notice in a place or manner reasonably likely to accomplish it.

(d) *Exceptions to submitter notice requirements.* The notice requirements of paragraphs (c) and (g) of this section shall not apply if:

(1) The component determines that the information is exempt under the FOIA;

(2) The information lawfully has been published or has been officially made available to the public;

(3) Disclosure of the information is required by a statute other than the FOIA or by a regulation issued in accordance with the requirements of Executive Order 12600 of June 23, 1987; or

(4) The designation made by the submitter under paragraph (b) of this section appears obviously frivolous, except that, in such a case, the component shall give the submitter written notice of any final decision to disclose the information and must provide that notice within a reasonable number of days prior to a specified disclosure date.

(e) *Opportunity to object to disclosure.*

(1) A component will specify a reasonable time period, but no fewer than 10 working days, within which the submitter must respond to the notice referenced above. If a submitter has any objections to disclosure, it should provide the component a detailed written statement that specifies all grounds for withholding the particular information under any exemption of the FOIA. In order to rely on Exemption 4 as basis for nondisclosure, the submitter must

## §5.8

explain why the information constitutes a trade secret, or commercial or financial information that is privileged or confidential.

(2) A submitter who fails to respond within the time period specified in the notice shall be considered to have no objection to disclosure of the information. Information received by the component after the date of any disclosure decision will not be considered by the component. Any information provided by a submitter under this subpart may itself be subject to disclosure under the FOIA.

(f) *Analysis of objections.* A component shall consider a submitter's objections and specific grounds for nondisclosure in deciding whether to disclose the requested information.

(g) *Notice of intent to disclose.* Whenever a component decides to disclose information over the objection of a submitter, the component shall provide the submitter written notice, which shall include:

(1) A statement of the reasons why each of the submitter's disclosure objections was not sustained;

(2) A description of the information to be disclosed; and

(3) A specified disclosure date, which shall be a reasonable time subsequent to the notice, but no fewer than 10 working days.

(h) *Notice of FOIA lawsuit.* Whenever a requester files a lawsuit seeking to compel the disclosure of confidential commercial information, the component shall promptly notify the submitter.

(i) *Requester notification.* The component shall notify a requester whenever it provides the submitter with notice and an opportunity to object to disclosure; whenever it notifies the submitter of its intent to disclose the requested information; and whenever a submitter files a lawsuit to prevent the disclosure of the information.

(j) *Scope.* This section shall not apply to any confidential commercial information provided to CBP by a business submitter. Section 5.12 applies to such information. Section 5.12 also defines "confidential commercial information" as used in this paragraph.

## 6 CFR Ch. I (1-1-20 Edition)

### § 5.8 Administrative appeals.

(a) *Requirements for filing an appeal.*

(1) A requester may appeal adverse determinations denying his or her request or any part of the request to the appropriate Appeals Officer. A requester may also appeal if he or she questions the adequacy of the component's search for responsive records, or believes the component either misinterpreted the request or did not address all aspects of the request (*i.e.*, it issued an incomplete response), or if the requester believes there is a procedural deficiency (*e.g.*, fees were improperly calculated). For the address of the appropriate component Appeals Officer, contact the applicable component FOIA liaison using the information in appendix I to this subpart, visit [www.dhs.gov/foia](http://www.dhs.gov/foia), or call 1-866-431-0486. An appeal must be in writing, and to be considered timely it must be post-marked or, in the case of electronic submissions, transmitted to the Appeals Officer within 90 working days 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. ET or EDT on the 90th working day. 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. To facilitate handling, the requester should mark both the letter and the envelope, or the transmittal line in the case of electronic transmissions "Freedom of Information Act Appeal."

(2) An adverse determination by the component appeals officer will be the final action of DHS.

(b) *Adjudication of appeals.* (1) The DHS Office of the General Counsel or its designee (*e.g.*, component Appeals Officers) is the authorized appeals authority for DHS;

(2) On receipt of any appeal involving classified information, the Appeals Officer shall consult with the Chief Security Officer, and take appropriate action to ensure compliance with 6 CFR part 7;

(3) If the appeal becomes the subject of a lawsuit, the Appeals Officer is not required to act further on the appeal.

(c) *Appeal decisions.* The decision on the appeal will be made in writing. A decision that upholds a component's determination will contain a statement that identifies the reasons for the affirmation, including any FOIA exemptions applied. The decision will provide the requester with notification of the statutory right to file a lawsuit and will inform the requester of the mediation services offered by the Office of Government Information Services, of the National Archives and Records Administration, as a non-exclusive alternative to litigation. Should the requester elect to mediate any dispute related to the FOIA request with the Office of Government Information Services, DHS and its components will participate in the mediation process in good faith. If the adverse decision is reversed or modified on appeal, in whole or in part, the requester will be notified in a written decision and the request will be thereafter be further processed in accordance with that appeal decision.

(d) *Time limit for issuing appeal decision.* The statutory time limit for responding to appeals is generally 20 working days after receipt. However, the Appeals Officer may extend the time limit for responding to an appeal provided the circumstances set forth in 5 U.S.C. 552(a)(6)(B)(i) are met.

(e) *Appeal necessary before seeking court review.* If a requester wishes to seek court review of a component's adverse determination on a matter appealable under paragraph (a)(1) of this section, the requester must generally first appeal it under this subpart. However, a requester is not required to first file an appeal of an adverse determination of a request for expedited processing prior to seeking court review.

### § 5.9 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 pursuant to title 44 of the United States Code or the General Records Schedule 4.2 and/or 14 of

the National Archives and Records Administration. Records will not be disposed of or destroyed while they are the subject of a pending request, appeal, or lawsuit under the FOIA.

### § 5.10 FOIA requests for information contained in a Privacy Act system of records.

(a) *Information subject to Privacy Act.*

(1) If a requester submits a FOIA request for information about him or herself that is contained in a Privacy Act system of records applicable to the requester (*i.e.*, the information contained in the system of records is retrieved by the component using the requester's name or other personal identifier, and the information pertains to an individual covered by the Privacy Act) the request will be processed under both the FOIA and the Privacy Act.

(2) If the information the requester is seeking is not subject to the Privacy Act (*e.g.*, the information is filed under another subject, such as an organization, activity, event, or an investigation not retrievable by the requester's name or personal identifier), the request, if otherwise properly made, will be treated only as a FOIA request. In addition, if the information is covered by the Privacy Act and the requester does not provide proper verification of the requester's identity, the request, if otherwise properly made, will be processed only under the FOIA.

(b) *When both Privacy Act and FOIA exemptions apply.* Only if both a Privacy Act exemption and a FOIA exemption apply can DHS withhold information from a requester if the information sought by the requester is about him or herself and is contained in a Privacy Act system of records applicable to the requester.

(c) *Conditions for release of Privacy Act information to third parties in response to a FOIA request.* If a requester submits a FOIA request for Privacy Act information about another individual, the information will not be disclosed without that person's prior written consent that provides the same verification information that the person would have been required to submit for information about him or herself, unless—

## §5.11

(1) The information is required to be released under the FOIA, as provided by 5 U.S.C. 552a (b)(2); or

(2) In most circumstances, if the individual is deceased.

(d) *Privacy Act requirements.* See DHS's Privacy Act regulations in 5 CFR part 5, subpart B for additional information regarding the requirements of the Privacy Act.

### §5.11 Fees.

(a) *In general.* Components shall charge for processing requests under the FOIA in accordance with the provisions of this section and with the OMB Guidelines. Components will ordinarily use the most efficient and least expensive method for processing requested records. In order to resolve any fee issues that arise under this section, a component may contact a requester for additional information. A component ordinarily will collect all applicable fees before sending copies of records to a requester. If you make a FOIA request, it shall be considered a firm commitment to pay all applicable fees charged under §5.11, up to \$25.00, unless you seek a waiver of fees. Requesters must pay fees by check or money order made payable to the Treasury of the United States.

(b) *Definitions.* Generally, "requester category" means one of the three categories in which agencies place requesters for the purpose of determining whether a requester will be charged fees for search, review and duplication; categories include commercial requesters, noncommercial scientific or educational institutions or news media requesters, and all other requesters. The term "fee waiver" means that processing fees will be waived, or reduced, if a requester can demonstrate that certain statutory standards are satisfied including that the information is in the public interest and is not requested for a primarily commercial interest. For purposes of this section:

(1) *Commercial use request* is a request that asks for information for a use or a purpose that furthers a commercial, trade, or profit interest, which can include furthering those interests through litigation. A component's decision to place a requester in the commercial use category will be made on a

## 6 CFR Ch. I (1-1-20 Edition)

case-by-case basis based on the requester's intended use of the information.

(2) *Direct costs* are those expenses that an agency expends in searching for and duplicating (and, in the case of commercial use requests, reviewing) records in order to respond to a FOIA request. For example, direct costs include the salary of the employee performing the work (*i.e.*, the basic rate of pay for the employee, plus 16 percent of that rate to cover benefits) and the cost of operating computers and other electronic equipment, such as photocopiers and scanners. Direct costs do not include overhead expenses such as the costs of space, and of heating or lighting a facility.

(3) *Duplication* is reproducing a copy of a record or of the information contained in it, necessary to respond to a FOIA request. Copies can take the form of paper, audiovisual materials, or electronic records, among others.

(4) *Educational institution* is any school that operates a program of scholarly research. A requester in this fee category must show that the request is made in connection with his or her role at the educational institution. Components may seek verification from the requester that the request is in furtherance of scholarly research.

*Example 1.* A request from a professor of geology at a university for records relating to soil erosion, written on letterhead of the Department of Geology, would be presumed to be from an educational institution if the request adequately describes how the requested information would further a specific research goal of the educational institution.

*Example 2.* A request from the same professor of geology seeking immigration information from the U.S. Immigration and Customs Enforcement in furtherance of a murder mystery he is writing would not be presumed to be an institutional request, regardless of whether it was written on institutional stationery.

*Example 3.* A student who makes a request in furtherance of their coursework or other school-sponsored activities and provides a copy of a course syllabus or other reasonable documentation to indicate the research purpose for the request, would qualify as part of this fee category.

NOTE: These examples are provided for guidance purposes only. Each individual request will be evaluated under the particular facts, circumstances, and information provided by the requester.

(5) *Noncommercial scientific institution* is an institution that is not operated on a “commercial” basis, as defined in paragraph (b)(1) of this section, and that is operated solely for the purpose of conducting scientific research the results of which are not intended to promote any particular product or industry. A requester in this category must show that the request is authorized by and is made under the auspices of a qualifying institution and that the records are sought to further scientific research and not for a commercial use.

(6) *Representative of the news media* is any person or entity that actively gathers information of potential interest to a segment of the public, uses its editorial skills to turn the raw materials into a distinct work, and distributes that work to an audience. The term “news” means information that is about current events or that would be of current interest to the public. Examples of news media entities include television or radio stations that broadcast “news” to the public at large and publishers of periodicals that disseminate “news” and make their products available through a variety of means to the general public, including but not limited to, news organizations that disseminate solely on the Internet. A request for records that supports the news-dissemination function of the requester shall not be considered to be for a commercial use. In contrast, data brokers or others who merely compile and market government information for direct economic return shall not be presumed to be news media entities. “Freelance” journalists must demonstrate a solid basis for expecting publication through a news media entity in order to be considered as working for a news media entity. A publication contract would provide the clearest evidence that publication is expected; however, components shall also consider a requester’s past publication record in making this determination.

(7) *Review* is the page-by-page, line-by-line examination of a record located in response to a request in order to determine whether any portion of it is exempt from disclosure. Review time includes processing any record for disclosure, such as doing all that is necessary to prepare the record for disclo-

sure, including the process of redacting the record and marking the appropriate exemptions. Review costs are properly charged even if a record ultimately is not disclosed. Review time also includes time spent both obtaining and considering any formal objection to disclosure made by a confidential commercial information submitter under § 5.7 or § 5.12, but it does not include time spent resolving general legal or policy issues regarding the application of exemptions.

(8) *Search* is the process of looking for and retrieving records or information responsive to a request. Search time includes page-by-page or line-by-line identification of information within records; and the reasonable efforts expended to locate and retrieve information from electronic records. Components shall ensure that searches are done in the most efficient and least expensive manner reasonably possible by readily available means.

(c) *Charging fees.* In responding to FOIA requests, components shall charge the following fees unless a waiver or reduction of fees has been granted under paragraph (k) of this section. Because the fee amounts provided below already account for the direct costs associated with a given fee type, unless otherwise stated in § 5.11, components should not add any additional costs to those charges.

(1) *Search.* (i) Search fees shall be charged for all requests subject to the restrictions of paragraph (d) of this section. Components may properly charge for time spent searching even if they do not locate any responsive records or if they determine that the records are entirely exempt from disclosure.

(ii) For each quarter hour spent by personnel searching for requested records, including electronic searches that do not require new programming, the fees will be as follows: Managerial—\$10.25; professional—\$7.00; and clerical/administrative—\$4.00.

(iii) Requesters will be charged the direct costs associated with conducting any search that requires the creation of a new computer program, as referenced in section 5.4, to locate the requested records. Requesters shall be notified of the costs associated with

## §5.11

## 6 CFR Ch. I (1–1–20 Edition)

creating such a program and must agree to pay the associated costs before the costs may be incurred.

(iv) For requests that require the retrieval of records stored by an agency at a federal records center operated by the National Archives and Records Administration (NARA), additional costs shall be charged in accordance with the Transactional Billing Rate Schedule established by NARA.

(2) *Duplication.* Duplication fees will be charged to all requesters, subject to the restrictions of paragraph (d) of this section. 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. Where photocopies are supplied, the component will provide one copy per request at a cost of ten cents per page. For copies of records produced on tapes, disks, or other media, components will charge the direct costs of producing the copy, including operator time. Where paper documents must be scanned in order to comply with a requester's preference to receive the records in an electronic format, the requester shall pay the direct costs associated with scanning those materials. For other forms of duplication, components will charge the direct costs.

(3) *Review.* Review fees will be charged to requesters who make commercial use requests. Review fees will be assessed in connection with the initial review of the record, *i.e.*, the review conducted by a component to determine whether an exemption applies to a particular record or portion of a record. No charge will be made for review at the administrative appeal stage of exemptions applied at the initial review stage. However, when the appellate authority determines that a particular exemption no longer applies, any costs associated with a component's re-review of the records in order to consider the use of other exemptions may be assessed as review fees. Review fees will be charged at the same rates as those charged for a search under paragraph (c)(1)(ii) of this section.

(d) *Restrictions on charging fees.* (1) No search fees will be charged for requests by educational institutions, non-

commercial scientific institutions, or representatives of the news media, unless the records are sought for a commercial use.

(2) If a component fails to comply with the FOIA's time limits in which to respond to a request, it may not charge search fees, or, in the instances of requests from requesters described in paragraph (d)(1) of this section, may not charge duplication fees, except as described in (d)(2)(i) through (iii).

(i) If a component has determined that unusual circumstances as defined by the FOIA apply and the component provided timely written notice to the requester in accordance with the FOIA, a failure to comply with the time limit shall be excused for an additional 10 days.

(ii) If a component has determined that unusual circumstances, as defined by the FOIA, apply and more than 5,000 pages are necessary to respond to the request, a component may charge search fees, or, in the case of requesters described in paragraph (d)(1) of this section, may charge duplication fees, if the following steps are taken. The component must have provided timely written notice of unusual circumstances to the requester in accordance with the FOIA and the component must have discussed with the requester via written mail, email, or telephone (or made not less than three good-faith attempts to do so) how the requester could effectively limit the scope of the request in accordance with 5. U.S.C. 552(a)(6)(B)(ii). If this exception is satisfied, the component may charge all applicable fees incurred in the processing of the request.

(iii) If a court has determined that exceptional circumstances exist, as defined by the FOIA, a failure to comply with the time limits shall be excused for the length of time provided by the court order.

(3) No search or review fees will be charged for a quarter-hour period unless more than half of that period is required for search or review.

(4) Except for requesters seeking records for a commercial use, components will provide without charge:

(i) The first 100 pages of duplication (or the cost equivalent for other media); and

(ii) The first two hours of search.

(5) When, after first deducting the 100 free pages (or its cost equivalent) and the first two hours of search, a total fee calculated under paragraph (c) of this section is \$14.00 or less for any request, no fee will be charged.

(e) *Notice of anticipated fees in excess of \$25.00.* (1) When a component determines or estimates that the fees to be assessed in accordance with this section will exceed \$25.00, the component shall notify the requester of the actual or estimated amount of the fees, including a breakdown of the fees for search, review and/or duplication, unless the requester has indicated a willingness to pay fees as high as those anticipated. If only a portion of the fee can be estimated readily, the component shall advise the requester accordingly. If the requester is a noncommercial use requester, the notice will specify that the requester is entitled to his or her statutory entitlements of 100 pages of duplication at no charge and, if the requester is charged search fees, two hours of search time at no charge, and will advise the requester whether those entitlements have been provided. Two hours of search time will be provided free of charge to non-commercial requesters regardless of whether they agree to pay estimated fees.

(2) In cases in which a requester has been notified that the actual or estimated fees are in excess of \$25.00, the request shall not be considered received and further work will not be completed until the requester commits in writing to pay the actual or estimated total fee, or designates some amount of fees he or she is willing to pay, or in the case of a noncommercial use requester who has not yet been provided with his or her statutory entitlements, designates that he or she seeks only that which can be provided by the statutory entitlements. The requester must provide the commitment or designation in writing, and must, when applicable, designate an exact dollar amount the requester is willing to pay. Components are not required to accept payments in installments.

(3) If the requester has indicated a willingness to pay some designated amount of fees, but the component estimates that the total fee will exceed

that amount, the component will toll the processing of the request while it notifies the requester of the estimated fees in excess of the amount the requester has indicated a willingness to pay. The component shall inquire whether the requester wishes to revise the amount of fees he or she is willing to pay and/or modify the request. Once the requester responds, the time to respond will resume from where it was at the date of the notification.

(4) Components will make available their FOIA Public Liaison or other FOIA professional to assist any requester in reformulating a request to meet the requester's needs at a lower cost.

(f) *Charges for other services.* Although not required to provide special services, if a component chooses to do so as a matter of administrative discretion, the direct costs of providing the service will be charged. Examples of such services include certifying that records are true copies, providing multiple copies of the same document, or sending records by means other than first class mail.

(g) *Charging interest.* Components may charge interest on any unpaid bill starting on the 31st day following the date of billing the requester. Interest charges will be assessed at the rate provided in 31 U.S.C. 3717 and will accrue from the billing date until payment is received by the component. Components will follow the provisions of the Debt Collection Act of 1982 (Pub. L. 97-365, 96 Stat. 1749), as amended, and its administrative procedures, including the use of consumer reporting agencies, collection agencies, and offset.

(h) *Aggregating requests.* When a component reasonably believes that a requester or a group of requesters acting in concert is attempting to divide a single request into a series of requests for the purpose of avoiding fees, the component may aggregate those requests and charge accordingly. Components may presume that multiple requests of this type made within a 30-day period have been made in order to avoid fees. For requests separated by a

## §5.11

## 6 CFR Ch. I (1–1–20 Edition)

longer period, components will aggregate them only where there is a reasonable basis for determining that aggregation is warranted in view of all the circumstances involved. Multiple requests involving unrelated matters will not be aggregated.

(i) *Advance payments.* (1) For requests other than those described in paragraphs (i)(2) and (3) of this section, a component shall not require the requester to make an advance payment before work is commenced or continued on a request. Payment owed for work already completed (*i.e.*, payment before copies are sent to a requester) is not an advance payment.

(2) When a component determines or estimates that a total fee to be charged under this section will exceed \$250.00, it may require that the requester make an advance payment up to the amount of the entire anticipated fee before beginning to process the request. A component may elect to process the request prior to collecting fees when it receives a satisfactory assurance of full payment from a requester with a history of prompt payment.

(3) Where a requester has previously failed to pay a properly charged FOIA fee to any component or agency within 30 calendar days of the billing date, a component may require that the requester pay the full amount due, plus any applicable interest on that prior request and the component may require that the requester make an advance payment of the full amount of any anticipated fee, before the component begins to process a new request or continues to process a pending request or any pending appeal. Where a component has a reasonable basis to believe that a requester has misrepresented his or her identity in order to avoid paying outstanding fees, it may require that the requester provide proof of identity.

(4) In cases in which a component requires advance payment, the request shall not be considered received and further work will not be completed until the required payment is received. If the requester does not pay the advance payment within 30 calendar days after the date of the component's fee determination, the request will be closed.

(j) *Other statutes specifically providing for fees.* The fee schedule of this section does not apply to fees charged under any statute that specifically requires an agency to set and collect fees for particular types of records. In instances where records responsive to a request are subject to a statutorily-based fee schedule program, the component will inform the requester of the contact information for that source.

(k) *Requirements for waiver or reduction of fees.* (1) Records responsive to a request shall be furnished without charge or at a reduced rate below that established under paragraph (c) of this section, where a component determines, on a case-by-case basis, based on all available information, that the requester has demonstrated that:

(i) Disclosure of the requested information is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government; and

(ii) Disclosure of the information is not primarily in the commercial interest of the requester.

(2) In deciding whether disclosure of the requested information is in the public interest because it is likely to contribute significantly to public understanding of operations or activities of the government, components will consider the following factors:

(i) The subject of the request must concern identifiable operations or activities of the federal government, with a connection that is direct and clear, not remote or attenuated.

(ii) Disclosure of the requested records must be meaningfully informative about government operations or activities in order to be “likely to contribute” to an increased public understanding of those operations or activities. The disclosure of information that already is in the public domain, in either the same or a substantially identical form, would not contribute to such understanding where nothing new would be added to the public's understanding.

(iii) The disclosure must contribute to the understanding of a reasonably broad audience of persons interested in the subject, as opposed to the individual understanding of the requester.

A requester's expertise in the subject area as well as his or her ability and intention to effectively convey information to the public shall be considered. It shall be presumed that a representative of the news media will satisfy this consideration.

(iv) The public's understanding of the subject in question must be enhanced by the disclosure to a significant extent. However, components shall not make value judgments about whether the information at issue is "important" enough to be made public.

(3) To determine whether disclosure of the requested information is primarily in the commercial interest of the requester, components will consider the following factors:

(i) Components shall identify any commercial interest of the requester, as defined in paragraph (b)(1) of this section, that would be furthered by the requested disclosure. Requesters shall be given an opportunity to provide explanatory information regarding this consideration.

(ii) A waiver or reduction of fees is justified where the public interest is greater than any identified commercial interest in disclosure. Components ordinarily shall presume that where a

news media requester has satisfied the public interest standard, the public interest will be the interest primarily served by disclosure to that requester. Disclosure to data brokers or others who merely compile and market government information for direct economic return shall not be presumed to primarily serve the public interest.

(4) Where only some of the records to be released satisfy the requirements for a waiver of fees, a waiver shall be granted for those records.

(5) Requests for a waiver or reduction of fees should be made when the request is first submitted to the component and should address the criteria referenced above. A requester may submit a fee waiver request at a later time so long as the underlying record request is pending or on administrative appeal. When a requester who has committed to pay fees subsequently asks for a waiver of those fees and that waiver is denied, the requester will be required to pay any costs incurred up to the date the fee waiver request was received.

(6) *Summary of fees.* The following table summarizes the chargeable fees (excluding direct fees identified in § 5.11) for each requester category.

Category	Search fees	Review fees	Duplication fees
Commercial-use .....	Yes .....	Yes .....	Yes.
Educational or Non-Commercial Scientific Institution.	No .....	No .....	Yes (100 pages free).
News Media .....	No .....	No .....	Yes (100 pages free).
Other requesters .....	Yes (2 hours free) .....	No .....	Yes (100 pages free).

**§ 5.12 Confidential commercial information; CBP procedures.**

(a) *In general.* For purposes of this section, "commercial information" is defined as trade secret, commercial, or financial information obtained from a person. Commercial information provided to CBP by a business submitter and that CBP determines is privileged or confidential commercial or financial information will be treated as privileged or confidential and will not be disclosed pursuant to a Freedom of Information Act request or otherwise made known in any manner except as provided in this section.

(b) *Notice to business submitters of FOIA requests for disclosure.* Except as provided in paragraph (b)(2) of this section, CBP will provide business submitters with prompt written notice of receipt of FOIA requests or appeals that encompass their commercial information. The written notice will describe either the exact nature of the commercial information requested, or enclose copies of the records or those portions of the records that contain the commercial information. The written notice also will advise the business submitter of its right to file a disclosure objection statement as provided under paragraph (c)(1) of this section. CBP

## §5.13

## 6 CFR Ch. I (1–1–20 Edition)

will provide notice to business submitters of FOIA requests for the business submitter's commercial information for a period of not more than 10 years after the date the business submitter provides CBP with the information, unless the business submitter requests, and provides acceptable justification for, a specific notice period of greater duration.

(1) *When notice is required.* CBP will provide business submitters with notice of receipt of a FOIA request or appeal whenever:

(i) The business submitter has in good faith designated the information as commercially- or financially-sensitive information. The business submitter's claim of confidentiality should be supported by a statement by an authorized representative of the business entity providing specific justification that the information in question is considered confidential commercial or financial information and that the information has not been disclosed to the public; or

(ii) CBP has reason to believe that disclosure of the commercial information could reasonably be expected to cause substantial competitive harm.

(2) *When notice is not required.* The notice requirements of this section will not apply if:

(i) CBP determines that the commercial information will not be disclosed;

(ii) The commercial information has been lawfully published or otherwise made available to the public; or

(iii) Disclosure of the information is required by law (other than 5 U.S.C. 552).

(c) *Procedure when notice given—(1) Opportunity for business submitter to object to disclosure.* A business submitter receiving written notice from CBP of receipt of a FOIA request or appeal encompassing its commercial information may object to any disclosure of the commercial information by providing CBP with a detailed statement of reasons within 10 days of the date of the notice (exclusive of Saturdays, Sundays, and legal public holidays). The statement should specify all the grounds for withholding any of the commercial information under any exemption of the FOIA and, in the case of Exemption 4, should demonstrate why

the information is considered to be a trade secret or commercial or financial information that is privileged or confidential. The disclosure objection information provided by a person pursuant to this paragraph may be subject to disclosure under the FOIA.

(2) *Notice to FOIA requester.* When notice is given to a business submitter under paragraph (b)(1) of this section, notice will also be given to the FOIA requester that the business submitter has been given an opportunity to object to any disclosure of the requested commercial information.

(d) *Notice of intent to disclose.* CBP will consider carefully a business submitter's objections and specific grounds for nondisclosure prior to determining whether to disclose commercial information. Whenever CBP decides to disclose the requested commercial information over the objection of the business submitter, CBP will provide written notice to the business submitter of CBP's intent to disclose, which will include:

(1) A statement of the reasons for which the business submitter's disclosure objections were not sustained;

(2) A description of the commercial information to be disclosed; and

(3) A specified disclosure date which will not be less than 10 days (exclusive of Saturdays, Sundays, and legal public holidays) after the notice of intent to disclose the requested information has been issued to the business submitter. Except as otherwise prohibited by law, CBP will also provide a copy of the notice of intent to disclose to the FOIA requester at the same time.

(e) *Notice of FOIA lawsuit.* Whenever a FOIA requester brings suit seeking to compel the disclosure of commercial information covered by paragraph (b)(1) of this section, CBP will promptly notify the business submitter in writing.

### §5.13 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 FOIA.

**Office of the Secretary, Homeland Security**

**Pt. 5, Subpt. A, App. I**

APPENDIX I TO SUBPART A TO PART 5—  
FOIA CONTACT INFORMATION

*Department of Homeland Security Chief FOIA  
Officer*

Chief Privacy Officer/Chief FOIA Officer, The Privacy Office, U.S. Department of Homeland Security, 245 Murray Lane SW., STOP-0655, Washington, DC. 20528-0655

*Department of Homeland Security Deputy Chief  
FOIA Officer*

Deputy Chief FOIA Officer, The Privacy Office, U.S. Department of Homeland Security, 245 Murray Lane SW., STOP-0655, Washington, DC 20528-0655

*Senior Director, FOIA Operations*

Sr. Director, FOIA Operations, The Privacy Office, U.S. Department of Homeland Security, 245 Murray Lane SW., STOP-0655, Washington, DC 20528-0655, Phone: 202-343-1743 or 866-431-0486, Fax: 202-343-4011, Email: [foia@hq.dhs.gov](mailto:foia@hq.dhs.gov)

*Director, FOIA Production and Quality  
Assurance*

Public Liaison, FOIA Production and Quality Assurance, The Privacy Office, U.S. Department of Homeland Security, 245 Murray Lane SW., STOP-0655, Washington, DC 20528-0655, Phone: 202-343-1743 or 866-431-0486, Fax: 202-343-4011, Email: [foia@hq.dhs.gov](mailto:foia@hq.dhs.gov)

*U.S. Customs & Border Protection (CBP)*

FOIA Officer/Public Liaison, 90 K Street NE., 9th Floor, Washington, DC 20229-1181, Phone: 202-325-0150, Fax: 202-325-0230

*Office of Civil Rights and Civil Liberties (CRCL)*

FOIA Officer/Public Liaison, U.S. Department of Homeland Security, Washington, DC 20528, Phone: 202-357-1218, Email: [CRCL@dhs.gov](mailto:CRCL@dhs.gov)

*Federal Emergency Management Agency  
(FEMA)*

FOIA Officer/Public Liaison, 500 C Street SW., Room 7NE, Washington, DC 20472, Phone: 202-646-3323, Email: [fema-foia@dhs.gov](mailto:fema-foia@dhs.gov)

*Federal Law Enforcement Training Center  
(FLETC)*

FOIA Officer/Public Liaison, Building #681, Suite 187B, Glynco, GA 31524, Phone: 912-267-3103, Fax: 912-267-3113, Email: [fletc-foia@dhs.gov](mailto:fletc-foia@dhs.gov)

*National Protection and Programs Directorate  
(NPPD)*

FOIA Officer/Public Liaison, U.S. Department of Homeland Security, Washington,

DC 20528, Phone: 703-235-2211, Fax: 703-235-2052, Email: [NPPD.FOIA@dhs.gov](mailto:NPPD.FOIA@dhs.gov)

Office of Biometric Identity Management (OBIM) FOIA Officer, Department of Homeland Security, Washington, DC 20598-0628, Phone: 202-298-5454, Fax: 202-298-5445, E-Mail: [OBIM-FOIA@ice.dhs.gov](mailto:OBIM-FOIA@ice.dhs.gov)

*Office of Intelligence & Analysis (I&A)*

FOIA Officer/Public Liaison, U.S. Department of Homeland Security, Washington, DC 20528, Phone: 202-447-4883, Fax: 202-612-1936, Email: [I&AFOIA@hq.dhs.gov](mailto:I&AFOIA@hq.dhs.gov)

*Office of Inspector General (OIG)*

FOIA Public Liaison, DHS-OIG Counsel, STOP 0305, 245 Murray Lane SW., Washington, DC 20528-0305, Phone: 202-254-4001, Fax: 202-254-4398, Email: [FOIA.OIG@oig.dhs.gov](mailto:FOIA.OIG@oig.dhs.gov)

*Office of Operations Coordination and Planning  
(OPS)*

FOIA Officer/Public Liaison, U.S. Department of Homeland Security, Washington, DC 20528, Phone: 202-447-4156, Fax: 202-282-9811, Email: [FOIAOPS@DHS.GOV](mailto:FOIAOPS@DHS.GOV)

*Science & Technology Directorate (S&T)*

FOIA Officer/Public Liaison, U.S. Department of Homeland Security, Washington, DC 20528, Phone: 202-254-6342, Fax: 202-254-6739, Email: [stfoia@hq.dhs.gov](mailto:stfoia@hq.dhs.gov)

*Transportation Security Administration (TSA)*

FOIA Officer/Public Liaison, Freedom of Information Act Branch, 601 S. 12th Street, 11th Floor, East Tower, TSA-20, Arlington, VA 20598-6020, Phone: 1-866-FOIA-TSA or 571-227-2300, Fax: 571-227-1406, Email: [foia.tsa@dhs.gov](mailto:foia.tsa@dhs.gov)

*U.S. Citizenship & Immigration Services  
(USCIS)*

FOIA Officer/Public Liaison, National Records Center, FOIA/PA Office, P.O. Box 648010, Lee's Summit, Mo. 64064-8010, Phone: 1-800-375-5283 (USCIS National Customer Service Unit), Fax: 816-350-5785, Email: [uscis.foia@uscis.dhs.gov](mailto:uscis.foia@uscis.dhs.gov)

*United States Coast Guard (USCG)*

Commandant (CG-611), 2100 2nd St., SW., Attn: FOIA Officer/Public Liaison, Washington, DC 20593-0001, FOIA Requester Service Center Contact: Amanda Ackerson, Phone: 202-475-3522, Fax: 202-475-3927, Email: [efoia@uscg.mil](mailto:efoia@uscg.mil)

*United States Immigration & Customs  
Enforcement (ICE)*

Freedom of Information Act Office, FOIA Officer/Public Liaison 500 12th Street, SW., Stop 5009, Washington, DC 20536-5009,

## § 5.20

FOIA Requester Service Center Contact, Phone: 866-633-1182, Fax: 202-732-4265, Email: [ice-foia@dhs.gov](mailto:ice-foia@dhs.gov)

*United States Secret Service (USSS)*

Freedom of Information and Privacy Acts Branch, FOIA Officer/Public Liaison, 245 Murray Drive, Building 410, Washington, DC 20223, Phone: 202-406-6370, Fax: 202-406-5586, Email: [FOIA@uss.s.dhs.gov](mailto:FOIA@uss.s.dhs.gov)

Please direct all requests for information from the Office of the Secretary, Citizenship and Immigration Services Ombudsman, Domestic Nuclear Detection Office, Office of the Executive Secretary, Office of Intergovernmental Affairs, Management Directorate, Office of Policy, Office of the General Counsel, Office of Health Affairs, Office of Legislative Affairs, Office of Public Affairs and the Privacy Office, to the DHS Privacy Office at:

The Privacy Office, U.S. Department of Homeland Security, 245 Murray Lane SW., STOP-0655, Washington, DC 20528-0655, Phone: 202-343-1743 or 866-431-0486, Fax: 202-343-4011, Email: [foia@hq.dhs.gov](mailto:foia@hq.dhs.gov)

### 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) follows under the Privacy Act of 1974 (5 U.S.C. 552a). These rules should be read together with the Privacy Act, which provides additional information about records maintained on individuals. The rules in this subpart apply to all records in systems of records maintained by the Department that are retrieved by an individual's name or personal identifier. 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 of those by the Department. In addition, the Department processes 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 this part, which gives requests the benefit of both statutes.

(2) The provisions established by this subpart shall apply to all Department components that are transferred to the Department. Except to the extent a Department component has adopted separate

## 6 CFR Ch. I (1–1–20 Edition)

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.

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

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

(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.

(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) exemption.* As a general matter, when applying the (b)(1) exemption for 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) exemption.

(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.* You may make a request for access to a Department of Homeland Security record about yourself by appearing in person or by writing directly to the Department component that maintains the record. Your request should be sent or delivered to the component's Privacy Act office at the address listed in appendix A to this part. In most cases, a component's central Privacy Act office is the place to send a Privacy Act request. For records held by a field office of the U.S. Customs Service, U.S. Secret Service, U.S. Coast Guard, or any other Department component with field offices, however, you must write directly to that Customs, Secret Service, Coast Guard, or other field office address, which can be found in most telephone books or by calling the component's central Privacy Act office. (The functions of each component are summarized elsewhere in this title and in the description of the Department and its components in the "United States Government Manual," which is issued annually and is available in most libraries, as well as for sale from the Government Printing Office's Superintendent of Documents. This manual also can be accessed electronically at the Government Printing Office's World Wide Web site (which can be found at [http://www.access.gpo.gov/su\\_docs](http://www.access.gpo.gov/su_docs)). Some records are maintained

under a government-wide systems of records notice, for example, Official Personnel Files are maintained under the authority of the Office of Personnel Management. In order to access records maintained under a government-wide notice, please send your request to the Privacy Act office of the original department or agency from which the component was transferred to the Department. If you cannot determine where within the Department to send your request, you may send it to the Departmental Disclosure Officer, Department of Homeland Security, Washington, DC 20528, and that office will forward it to the component(s) it believes most likely to have the records that you seek. For the quickest possible handling, you should mark both your request letter and the envelope "Privacy Act Request."

(b) *Description of records sought.* You must describe the records that you want in enough detail to enable Department personnel to locate the system of records containing them with a reasonable amount of effort. Whenever possible, your request should describe the records sought, the time periods in which you believe they were compiled, and the name or identifying number of each system of records in which you believe they are kept. The Department publishes notices in the FEDERAL REGISTER that describe its components' systems of records. A description of the Department's systems of records also may be found as part of the "Privacy Act Compilation" published by the National Archives and Records Administration's Office of the Federal Register. This compilation is available in most large reference and university libraries. This compilation also can be accessed electronically at the Government Printing Office's World Wide Web site (which can be found at [http://www.access.gpo.gov/su\\_docs](http://www.access.gpo.gov/su_docs)).

(c) *Agreement to pay fees.* If you make a Privacy Act request for access to records, it shall be considered an agreement by you to pay all applicable fees charged under § 5.29, up to \$25.00. The component responsible for responding

## §5.22

to your request ordinarily shall confirm this agreement in an acknowledgement letter. When making a request, you may specify a willingness to pay a greater or lesser amount.

(d) *Verification of identity.* When you make a request for access to records about yourself, you must verify your identity. You must state your full name, current address, and date and place of birth. You must sign your request and your signature must either be notarized or submitted by you under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Departmental Disclosure Officer, Department of Homeland Security, Washington, DC 20528. In order to help the identification and location of requested records, you may also, at your option, include your social security number.

(e) *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 to be incompetent, for access to records about that individual, you 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, at your option, the social security number of the individual;

(2) Your own identity, as required in paragraph (d) of this section;

(3) That you are the parent or guardian of that individual, which you may prove by providing a copy of the individual's birth certificate showing your parentage or by providing a court order establishing your guardianship; and

(4) That you are acting on behalf of that individual in making the request.

(f) *Verification in the case of third party information requests.* If you are making a request for records concerning an individual on behalf of that individual, you must provide a statement from the individual verifying the identity of the individual as provided in paragraph (d) of this section. You must also provide a statement from the individual certifying the individual's

## 6 CFR Ch. I (1-1-20 Edition)

agreement that records concerning the individual may be released to you.

### §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 shall 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 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 request for access or amendment to a record of that component.

(c) *Consultations and referrals.* When a component receives a 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 either:

(1) Respond to the request regarding that record, after consulting with the component or agency best able to determine whether the record is exempt from access and with any other component or agency that has a substantial interest in it; or

(2) Refer the responsibility for responding to the request regarding that record to the component best able to determine whether it is exempt from access, or to another agency that originated the record (but only if that agency is subject to the Privacy Act). Ordinarily, the component or agency that originated a record will be presumed to be best able to determine whether it is exempt from access.

(d) *Law enforcement information.* Whenever a request is made for access to a record containing information that relates to an investigation of a possible violation of law and that was originated by another component or agency, 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.

(e) *Classified information.* 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 Executive Order 12958 or any other executive order concerning the classification of records, the receiving component shall refer the responsibility for responding to the request regarding that information to the component or agency that classified the information, should consider the information for classification, or has the primary interest in it, as appropriate. Whenever a record contains information that has been derivatively classified by a component because it contains information classified by another component or agency, the component shall refer the responsibility for responding to the request regarding that information to the component or agency that classified the underlying information.

(f) *Release of Medical Records.* Pursuant to 5 U.S.C. 552a(f)(3), where requests are made for access to medical records, including psychological records, the decision to release directly to the individual, or to withhold direct release, shall be made by a medical practitioner. Where the medical practitioner has ruled that direct release will cause harm to the individual who is requesting access, normal release through the individual's chosen medical practitioner will be recommended. Final review and decision on appeals of disapprovals of direct release will rest with the General Counsel.

(g) *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 shall 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.

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

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

#### § 5.23 Responses to requests for access to records.

(a) *Acknowledgements of requests.* On receipt of a request, a component ordinarily shall send an acknowledgement letter to the requester which shall confirm the requester's agreement to pay fees under § 5.21(c) and provide an assigned request number for further reference.

(b) *Grants of requests for access.* Once a component makes a determination to grant a 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 § 5.29 and shall disclose records to the requester promptly on payment of any applicable fee. If a request is made in person, the component may disclose records to the requester directly, in a manner not unreasonably disruptive of its operations, on payment of any applicable fee and with a written record made of the grant of the request. If a requester is accompanied by another person, the requester shall be required to authorize in writing any discussion of the records in the presence of the other person.

(c) *Adverse determinations of requests for access.* A component making an adverse determination denying a request for access in any respect shall notify the requester of that determination in writing. Adverse determinations, or denials of requests, consist of: a determination to withhold any requested record in whole or in part; a determination that a requested record does not exist or cannot be located; a determination that what has been requested

## §5.24

## 6 CFR Ch. I (1–1–20 Edition)

is not a record subject to the Privacy Act; a determination on any disputed fee matter; and a denial of a request for expedited treatment. The notification letter 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 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 §5.25(a) and a description of the requirements of §5.25(a).

### §5.24 Classified information.

In processing a request for access to a record containing information that is classified under Executive Order 12958 or any other executive order, the originating component shall review the information to determine whether it should remain classified. Information determined to no longer require classification shall not be withheld from a requester on the basis of Exemption (k)(1) of the Privacy Act. On receipt of any appeal involving classified information, the Associate General Counsel (General Law), shall take appropriate action to ensure compliance with part 7 of this title.

### §5.25 Appeals.

(a) *Appeals.* If you are dissatisfied with a component's response to your request for access to records, you may appeal an adverse determination denying your request in any respect to the Associate General Counsel (General Law), Department of Homeland Security, Washington, DC 20528. You must make your appeal in writing and it must be received by the Associate General Counsel (General Law) within 60 days of the date of the letter denying your request. Your appeal letter may include as much or as little related information as you wish, as long as it clearly identifies the component determination (including the assigned request number, if known) that you are appealing. For the quickest possible handling, you should mark both your appeal letter and the envelope "Privacy Act Appeal."

(b) *Responses to appeals.* The decision on your appeal will be made in writing. 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 you 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, you will be notified in a written decision and your request will be reprocessed in accordance with that appeal decision. An adverse determination by the Associate General Counsel (General Law) will be the final action of the Department.

(c) *When appeal is required.* If you wish to seek review by a court of any adverse determination or denial of a request, you must first appeal it under this section. 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, you may make a request for amendment or correction of a record of the Department about you by writing directly to the Department component that maintains the record, following the procedures in §5.21. Your request should identify each particular record in question, state the amendment or correction that you want, and state why you believe that the record is not accurate, relevant, timely, or complete. You may submit any documentation that you think would be helpful. If you believe that the same record is in more than one system of records, you should state that and address your request to each component that maintains a system of records containing the record.

(b) *Component responses.* Within ten working days of receiving your request for amendment or correction of records, a component shall send you a written acknowledgment of its receipt of your request, and it shall promptly notify you whether your request is granted or denied. If the component grants your request in whole or in part,

it shall describe the amendment or correction made and shall advise you of your right to obtain a copy of the corrected or amended record, in disclosable form. If the component denies your request in whole or in part, it shall send you a letter signed by the head of the component, or the component head's designee, that shall 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 your appeal.

(c) *Appeals.* You may appeal a denial of a request for amendment or correction to the Associate General Counsel (General Law) in the same manner as a denial of a request for access to records (see § 5.25) and the same procedures shall be followed. If your appeal is denied, you shall be advised of your right to file a Statement of Disagreement as described in paragraph (d) of this section and of your right under the Privacy Act for court review of the decision.

(d) *Statements of Disagreement.* If your appeal under this section is denied in whole or in part, you have the right to file a Statement of Disagreement that states your reason(s) for disagreeing with the Department's denial of your 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. Your 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 and 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.

(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 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 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 Privacy Act (5 U.S.C. 552a(j) or (k)) by notice 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) of this section), you 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 you. 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. Your request for an accounting should identify each particular record in question and should be made by writing directly to the Department component that maintains the record, following the procedures in § 5.21.

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

(1) Disclosures for which accountings are not required to be kept, such as disclosures that are made to employees within the agency and disclosures that are made under the FOIA;

(2) Disclosures made to law enforcement agencies for authorized law enforcement activities in response to

## § 5.28

written requests from those law enforcement agencies specifying the law enforcement activities for which the disclosures are sought; or

(3) Disclosures made from law enforcement systems of records that have been exempted from accounting requirements.

(c) *Appeals.* You may appeal a denial of a request for an accounting to the Associate General Counsel (General Law) in the same manner as a denial of a request for access to records (see § 5.25) 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 14. Records will not be disposed of while they are the subject of a pending request, appeal, or lawsuit under the Act.

## § 5.29 Fees.

(a) Components shall charge fees for duplication of records under the Privacy Act in the same way in which they charge duplication fees under § 5.11.

(b) The Department shall not process a request under the Privacy Act from persons with an unpaid fee from any previous Privacy Act 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 a record pertaining to an individual is required to be disclosed by a court order, the component shall make reasonable efforts to provide notice of this to the individual. Notice shall 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 shall be given only after the order becomes public. This notice shall be mailed to the individual's last known address and shall contain a copy of the

## 6 CFR Ch. I (1-1-20 Edition)

order and a description of the information disclosed. Notice shall not be given if disclosure is made from a criminal law enforcement 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.

## § 5.31 Security of systems of records.

(a) *In general.* Each component shall 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 shall correspond to the sensitivity of the records that the controls protect. At a minimum, each component's administrative and physical controls shall 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 shall have 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.

**§ 5.32 Contracts for the operation of record systems.**

Under 5 U.S.C. 552a(m), any approved contract for the operation of a record system will contain the standard contract requirements issued by the General Services Administration to ensure compliance with the requirements of the Privacy Act for that record 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 shall ensure that employees authorized to collect information are aware:

(a) That individuals may not be denied any right, benefit, or privilege as a result 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.

**§ 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. Unless otherwise permitted by law, 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 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 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 unauthorized or inadvertent disclosure of a record to anyone.

**§ 5.35 Sanctions and penalties.**

Under the provisions of the Privacy Act, 5 U.S.C. 552a, civil and criminal penalties may be assessed.

**§ 5.36 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.

### Subpart C—Disclosure of Information in Litigation

SOURCE: 68 FR 4070, Jan. 27, 2003, unless otherwise noted.

#### § 5.41 Purpose and scope; definitions.

(a) This subpart C sets forth the procedures to be followed with respect to:

(1) Service of summonses and complaints or other requests or demands directed to the Department of Homeland Security (Department) or to any Department employee or former employee in connection with federal or state litigation arising out of or involving the performance of official activities of the Department; and

(2) The oral or written disclosure, in response to subpoenas, orders, or other requests or demands of federal or state judicial or quasi-judicial or administrative authority as well as state legislative authorities (collectively, “demands”), whether civil or criminal in nature, or in response to requests for depositions, affidavits, admissions, responses to interrogatories, document production, interviews, or other litigation-related matters, including pursuant to the Federal Rules of Civil Procedure, the Federal Rules of Criminal Procedure, or applicable state rules (collectively, “requests”), of any material contained in the files of the Department, any information relating to material contained in the files of the Department, or any information acquired while the subject of the demand or request is or was employed by the Department, or served as Secretary of the Department, as part of the performance of that person’s duties or by virtue of that person’s official status.

(b) The provisions established by this subpart shall apply to all Department components that are transferred to the Department. Except to the extent a Department component has adopted separate guidance governing the subject matter of a provision of this subpart, the provisions of this subpart shall apply to each component of the Department. Departmental components may issue their own guidance under this subpart subject to the approval of the General Counsel of the Department.

(c) For purposes of this subpart, and except as the Department may other-

wise determine in a particular case, the term employee includes all former Secretaries of Homeland Security and all employees of the Department of Homeland Security or other federal agencies who are or were appointed by, or subject to the supervision, jurisdiction, or control of the Secretary of Homeland Security, whether residing or working in the United States or abroad, including United States nationals, foreign nationals, and contractors. The procedures established within this subpart also apply to former employees of the Department where specifically noted.

(d) For purposes of this subpart, the term litigation encompasses all pre-trial, trial, and post-trial stages of all judicial or administrative actions, hearings, investigations, or similar proceedings before courts, commissions, boards (including the Board of Appellate Review), grand juries, or other judicial or quasi-judicial bodies or tribunals, whether criminal, civil, or administrative in nature. This subpart governs, *inter alia*, responses to discovery requests, depositions, and other pre-trial, trial, or post-trial proceedings, as well as responses to informal requests by attorneys or others in situations involving litigation. However, this subpart shall not apply to any claims against the Department by Department of Homeland Security employees (present or former), or applicants for Department employment, for which jurisdiction resides with the U.S. Equal Employment Opportunity Commission; the U.S. Merit Systems Protection Board; the Office of Special Counsel; the Federal Labor Relations Authority; the Foreign Service Labor Relations Board; the Foreign Service Grievance Board; or a labor arbitrator operating under a collective bargaining agreement between the Department and a labor organization representing Department employees; or their successor agencies or entities.

(e) For purposes of this subpart, official information means all information of any kind, however stored, that is in the custody and control of the Department, relates to information in the custody and control of the Department, or was acquired by Department employees, or former employees, as part of their official duties or because of

their official status within the Department while such individuals were employed by or served on behalf of the Department.

(f) Nothing in this subpart affects disclosure of information under the Freedom of Information Act (FOIA), 5 U.S.C. 552, the Privacy Act, 5 U.S.C. 552a, Executive Order 12958 on national security information (3 CFR, 1995 Comp., p. 333), the Government in the Sunshine Act, 5 U.S.C. 552b, the Department's implementing regulations or pursuant to congressional subpoena. Nothing in this subpart permits disclosure of information by the Department, its present and former employees, or the Secretary, that is protected or prohibited by statute or other applicable law.

(g) This subpart is intended only to inform the public about Department procedures concerning the service of process and responses to demands or requests and is not intended to and does not create, and may not be relied upon to create any right or benefit, substantive or procedural, enforceable at law by a party against the Department or the United States.

(h) Nothing in this subpart affects the rules and procedures, under applicable U.S. law and international conventions, governing diplomatic and consular immunity.

(i) Nothing in this subpart affects the disclosure of official information to other federal agencies or Department of Justice attorneys in connection with litigation conducted on behalf or in defense of the United States, its agencies, officers, and employees, or litigation in which the United States has an interest; or to federal, state, local, or foreign prosecuting and law enforcement authorities in conjunction with criminal law enforcement investigations, prosecutions, or other proceedings, e.g., extradition, deportation.

#### **§ 5.42 Service of summonses and complaints.**

(a) Only the Office of the General Counsel is authorized to receive and accept on behalf of the Department summonses or complaints sought to be served upon the Department, the Secretary, or Department employees. All such documents should be delivered or

addressed to the Office of the General Counsel, United States Department of Homeland Security, Washington, DC, 20528. The authorization for receipt shall in no way affect the requirements of service elsewhere provided in applicable rules and regulations.

(b) In the event any summons or complaint described in § 5.41(a) is delivered to an employee of the Department other than in the manner specified in this part, the recipient thereof shall decline to accept the proffered service and may notify the person attempting to make service of the Departmental regulations set forth herein.

(c) Except as otherwise provided §§ 5.42(d) and 5.43(c), the Department is not an authorized agent for service of process with respect to civil litigation against Department employees purely in their personal, non-official capacity. Copies of summonses or complaints directed to Department employees in connection with legal proceedings arising out of the performance of official duties may, however, be served upon the Office of the General Counsel.

(d) Although the Department is not an agent for the service of process upon its employees with respect to purely personal, non-official litigation, the Department recognizes that its employees should not use their official positions to evade their personal obligations and will, therefore, counsel and encourage Department employees to accept service of process in appropriate cases.

(e) Documents for which the Office of the General Counsel accepts service in official capacity only shall be stamped "Service Accepted in Official Capacity Only". Acceptance of service shall not constitute an admission or waiver with respect to jurisdiction, propriety of service, improper venue, or any other defense in law or equity available under applicable laws or rules.

#### **§ 5.43 Service of subpoenas, court orders, and other demands or requests for official information or action.**

(a) Except in cases in which the Department is represented by legal counsel who have entered an appearance or

#### §5.44

#### 6 CFR Ch. I (1–1–20 Edition)

otherwise given notice of their representation, only the Office of the General Counsel is authorized to receive and accept subpoenas, or other demands or requests directed to the Secretary, the Department, or any component thereof, or its employees, whether civil or criminal in nature, for:

(1) Material, including documents, contained in the files of the Department;

(2) Information, including testimony, affidavits, declarations, admissions, responses to interrogatories, or informal statements, relating to material contained in the files of the Department or which any Department employee acquired in the course and scope of the performance of his official duties;

(3) Garnishment or attachment of compensation of current or former employees; or

(4) The performance or non-performance of any official Department duty.

(b) In the event that any subpoena, demand, or request is sought to be delivered to a Department employee other than in the manner prescribed in paragraph (a) of this section, such employee shall, after consultation with the Office of the General Counsel, decline service and direct the server of process to the Departmental regulations. If the subpoena, demand, or other request is nonetheless delivered to the employee, the employee shall immediately forward a copy of that document to the Office of the General Counsel.

(c) Except as otherwise provided in this subpart, the Department is not an agent for service, or otherwise authorized to accept on behalf of its employees, any subpoenas, show-cause orders, or similar compulsory process of federal or state courts, or requests from private individuals or attorneys, which are not related to the employees' official duties except upon the express, written authorization of the individual Department employee to whom such demand or request is directed.

(d) Acceptance of such documents by the Office of the General Counsel does not constitute a waiver of any defenses that might otherwise exist with respect to service under the Federal Rules of Civil or Criminal Procedure or other applicable rules.

(e) Copies of any subpoenas, show cause orders, or similar compulsory process of federal or state courts, or requests from private individuals or attorneys, directed to former employees of the Department in connection with legal proceedings arising out of the performance of official duties shall also be served upon the Office of the General Counsel. The Department shall not, however, serve as an agent for service for the former employee, nor is the Department otherwise authorized to accept service on behalf of its former employees. If the demand involves their official duties, former employees who receive subpoenas, show cause orders, or similar compulsory process of federal or state courts should also notify in the component of the Department in which they were employed if the service involves their official duties while so employed.

(f) If the subpoena, demand, or other request is nonetheless delivered to the employee, the employee shall immediately forward a copy of that document to the Office of the General Counsel.

#### **§5.44 Testimony and production of documents prohibited unless approved by appropriate Department officials.**

(a) No employee, or former employee, of the Department shall, in response to a demand or request, including in connection with any litigation, provide oral or written testimony by deposition, declaration, affidavit, or otherwise concerning any information acquired while such person is or was an employee of the Department as part of the performance of that person's official duties or by virtue of that person's official status, unless authorized to do so by the Office of the General Counsel, or as authorized in §5.44(b).

(b) No employee, or former employee, shall, in response to a demand or request, including in connection with any litigation, produce any document or any material acquired as part of the performance of that employee's duties or by virtue of that employee's official status, unless authorized to do so by the Office of the General Counsel or the delegates thereof, as appropriate.

**§ 5.45 Procedure when testimony or production of documents is sought; general.**

(a) If official information is sought, through testimony or otherwise, by a request or demand, the party seeking such release or testimony must (except as otherwise required by federal law or authorized by the Office of the General Counsel) set forth in writing, and with as much specificity as possible, the nature and relevance of the official information sought. Where documents or other materials are sought, the party should provide a description using the types of identifying information suggested in § 5.3(b). Subject to § 5.47, Department employees may only produce, disclose, release, comment upon, or testify concerning those matters which were specified in writing and properly approved by the appropriate Department official designated in § 5.44. See *United States ex rel. Touhy v. Ragen*, 340 U.S. 462 (1951). The Office of the General Counsel may waive the requirement of this subsection in appropriate circumstances.

(b) To the extent it deems necessary or appropriate, the Department may also require from the party seeking such testimony or documents a plan of all reasonably foreseeable demands, including but not limited to the names of all employees and former employees from whom discovery will be sought, areas of inquiry, expected duration of proceedings requiring oral testimony, and identification of potentially relevant documents.

(c) The appropriate Department official designated in § 5.42 will notify the Department employee and such other persons as circumstances may warrant of its decision regarding compliance with the request or demand.

(d) The Office of the General Counsel will consult with the Department of Justice regarding legal representation for Department employees in appropriate cases.

**§ 5.46 Procedure when response to demand is required prior to receiving instructions.**

(a) If a response to a demand is required before the appropriate Department official designated in § 5.44 renders a decision, the Department, if nec-

essary, will request that the Department of Justice or the appropriate Department attorney take appropriate steps to stay, postpone, or obtain relief from the demand pending decision. If necessary, the attorney will:

(1) Appear with the employee upon whom the demand has been made;

(2) Furnish the court or other authority with a copy of the regulations contained in this subpart;

(3) Inform the court or other authority that the demand has been, or is being, as the case may be, referred for the prompt consideration of the appropriate Department official; and

(4) Respectfully request the court or authority to stay the demand pending receipt of the requested instructions.

(b) In the event that an immediate demand for production or disclosure is made in circumstances which would preclude the proper designation or appearance of a Department of Justice or appropriate Department attorney on the employee's behalf, the employee, if necessary, shall respectfully request from the demanding court or authority for a reasonable stay of proceedings for the purpose of obtaining instructions from the Department.

**§ 5.47 Procedure in the event of an adverse ruling.**

If a stay of, or other relief from, the effect of the demand in response to a request made pursuant to § 5.46 is declined or not obtained, or if the court or other judicial or quasi-judicial authority declines to stay the effect of the demand in response to a request made pursuant to § 5.46, or if the court or other authority rules that the demand must be complied with irrespective of the Department's instructions not to produce the material or disclose the information sought, the employee upon whom the demand has been made shall respectfully decline to comply with the demand, citing this subpart and *United States ex rel. Touhy v. Ragen*, 340 U.S. 462 (1951).

**§ 5.48 Considerations in determining whether the Department will comply with a demand or request.**

(a) In deciding whether to comply with a demand or request, Department officials and attorneys shall consider,

**§5.49**

**6 CFR Ch. I (1-1-20 Edition)**

among any other pertinent considerations:

(1) Whether such compliance would be unduly burdensome or otherwise inappropriate under the applicable rules of discovery or the rules of procedure governing the case or matter in which the demand arose;

(2) Whether compliance is appropriate under the relevant substantive law concerning privilege or disclosure of information;

(3) The public interest;

(4) The need to conserve the time of Department employees for the conduct of official business;

(5) The need to avoid spending the time and money of the United States for private purposes;

(6) The need to maintain impartiality between private litigants in cases where a substantial government interest is not implicated;

(7) Whether compliance would have an adverse effect on performance by the Department of its mission and duties; and

(8) The need to avoid involving the Department in controversial issues not related to its mission.

(b) Among those demands and requests in response to which compliance will not ordinarily be authorized are those with respect to which any of the following factors, *inter alia*, exist:

(1) Compliance would violate a statute or a rule of procedure;

(2) Compliance would violate a specific regulation or Executive order;

(3) Compliance would reveal information properly classified in the interest of national security;

(4) Compliance would reveal confidential commercial or financial information or trade secrets without the owner's consent;

(5) Compliance would reveal the internal deliberative processes of the Executive Branch; or

(6) Compliance would potentially impede or prejudice an on-going law enforcement investigation.

**§ 5.49 Prohibition on providing expert or opinion testimony.**

(a) Except as provided in this section, and subject to 5 CFR 2635.805, Department employees shall not provide opinion or expert testimony based upon in-

formation which they acquired in the scope and performance of their official Department duties, except on behalf of the United States or a party represented by the Department of Justice.

(b) Any expert or opinion testimony by a former employee of the Department shall be excepted from 5.49(a) where the testimony involves only general expertise gained while employed at the Department.

(c) Upon a showing by the requestor of exceptional need or unique circumstances and that the anticipated testimony will not be adverse to the interests of the United States, the appropriate Department official designated in §5.44 may, consistent with 5 CFR 2635.805, in their discretion and with the concurrence of the Office of the General Counsel, grant special, written authorization for Department employees, or former employees, to appear and testify as expert witnesses at no expense to the United States.

(d) If, despite the final determination of the appropriate Department official designated in §5.44, a court of competent jurisdiction or other appropriate authority orders the appearance and expert or opinion testimony of a current or former Department employee, that person shall immediately inform the Office of the General Counsel of such order. If the Office of the General Counsel determines that no further legal review of or challenge to the court's order will be made, the Department employee, or former employee, shall comply with the order. If so directed by the Office of the General Counsel, however, the employee, or former employee, shall respectfully decline to testify.

**APPENDIX A TO PART 5—FOIA/PRIVACY ACT OFFICES OF THE DEPARTMENT OF HOMELAND SECURITY**

I. For the following Headquarters components of the Department of Homeland Security, FOIA and Privacy Act requests should be sent to the Departmental Disclosure Office, Department of Homeland Security, Washington, DC 20528. The Headquarters components are:

## Office of the Secretary, Homeland Security

## Pt. 5, App. A

### A

Office of the Secretary  
Office of the Deputy Secretary  
Office of the Under Secretary for Management

### B

Office of the General Counsel  
Office of the Inspector General  
Office of International Affairs  
Office of Legislative Affairs  
Office of Public Affairs  
Office of National Capital Region Coordination  
Office of Professional Responsibility  
Office for State and Local Government Coordination

### C

Directorate of Border and Transportation Security  
Directorate of Emergency Preparedness and Response  
Directorate of Information Analysis and Infrastructure Protection  
Directorate of Science and Technology

II. Requests made to components that have transferred or will transfer into the Department of Homeland Security, should be sent as follows:

A. Former components of the Department of Agriculture:

1. Animal and Plant Health Inspection Service, USDA, APHIS, LPA, FOIA, 4700 River Road, Unit 50, Riverdale, MD 20737-1232
2. Plum Island Animal Disease Center; Submit request to the APHIS address above or, FOIA Coordinator, USDA-REE-ARS-Information Staff, 5601 Sunnyside Avenue, Bldg. 1, Room 2248, Mail Stop 5128, Beltsville, MD 20705-5128

B. Former components of the Department of Commerce:

1. Critical Infrastructure Assurance Office (A former office of the Bureau of Industry and Security); Freedom of Information Coordinator, Bureau of Industry and Security, Room 6883, U.S. Department of Commerce, Washington, DC 20230
2. FIRESTAT (formerly the Integrated Hazard Information System of the National Oceanic and Atmospheric Administration), National Oceanic and Atmospheric Administration, Public Reference Facility (OFAx2), 1315 East-West Highway (SSMC3), Room 10703, Silver Spring, MD 20910

C. Former components of the Department of Defense:

1. National Communications Service (A former component of the Defense Information Systems Agency), Defense Information Systems Agency, ATTN: RGC/FOIA Officer, 701 S. Courthouse Rd., Arlington, VA 22204-2199

D. Former components and programs of the Department of Energy:

The address for each component and program listed below is: U.S. Department of Energy, 1000 Independence Avenue, SW., Washington, DC 20585

1. Energy Assurance Office
2. Environmental Measurements Laboratory
3. Nuclear Incident Response Team
4. The chemical and biological national security and supporting programs and activities of the non-proliferation and verification research and development program.
5. The life sciences activities related to microbial pathogens of Biological and Environmental Research Program.
6. The nuclear smuggling programs and activities within the proliferation detection program of the non-proliferation and verification research and development program.
7. The nuclear assessment program and activities of the assessment, detection, and cooperation program of the international materials protection and cooperation program, and the advanced scientific computing research program and activities at Lawrence Livermore National Laboratory.
8. National Infrastructure Simulation and Analysis Center

E. Former components of the Department of Health and Human Services:

1. The address for each component and program listed below is: Department of Health and Human Services, Freedom of Information Officer, Room 645-F, Hubert H. Humphrey Building, Independence Avenue, SW., Washington, DC 20201;
  - a. Metropolitan Medical Response System,
  - b. National Disaster Medical System, and
  - c. Office of Emergency Preparedness
  - d. Strategic National Stockpile
2. Centers for Disease Control and Agency for Toxic Substances and Disease Registry, Attn: FOI Office, MS-D54, 1600 Clifton Road, NE., Atlanta, GA 30333.

F. Former components of the Department of Justice:

1. Immigration and Naturalization Service, Director, Freedom of Information/Privacy Act Program, Department of Justice, 425 Eye Street, NW., 2nd Floor, ULLICO Building, Washington, DC 20536 (for field offices, consult your phone book).
2. The address for each component and program listed below is: Federal Bureau of Investigation, Chief, FOIPA Section, 935 Pennsylvania Avenue, NW., Department of Justice, Washington, DC 20535-0001;
  - a. National Infrastructure Protection Center,
  - b. National Domestic Preparedness Office, and
  - c. Domestic Emergency Support Team.

## Pt. 5, App. C

## 6 CFR Ch. I (1–1–20 Edition)

3. Office of Domestic Preparedness, U.S. Department of Justice, Office of Justice Programs, Office of the General Counsel, Attention: FOIA Staff, 810 7th Street, NW., Room 5400, Washington, DC 20531.

G. Former components of the Department of State:

Visa Office, Information and Privacy Coordinator, Office of Information Resources, Management Programs and Services, A/RPS/IPS, SA-2, Department of State, Washington, DC 20522-6001, Re: Freedom of Information Act Request.

H. Former components of the Department of Transportation:

1. Federal Aviation Administration, National Freedom of Information Act Staff, ARC-40, 800 Independence Avenue, SW., Washington, DC 20591 (for regional centers, consult your phone book).
2. Transportation Security Administration, TSA-1, FOIA Division, 400 Seventh Street, SW., Washington, DC 20590
3. United States Coast Guard, HQ USCG Commandant, G-CIM, 2100 Second Street, SW., Washington, DC 20593-0001 (for district offices, consult your phone book).

I. Former components of the Department of Treasury:

1. Federal Law Enforcement Training Center, Freedom of Information Act Officer, Townhouse 389, Glynco, GA 31524
2. U.S. Customs Service, Freedom of Information Act Request, Mint Annex, 1300 Pennsylvania Avenue, NW., Washington, DC 20229 (for field offices, consult your phone book).
3. U.S. Secret Service, Freedom of Information Act Request, 950 H Street, NW., Suite 3000, Washington, DC 20223, e-mail [FOIA@USSS.Treas.gov](mailto:FOIA@USSS.Treas.gov). Appeals should be addressed to the Deputy Director, United States Secret Service, Freedom of Information and Privacy Act Appeal Officer, at these same contact points.

J. Federal Emergency Management Agency: Federal Emergency Management Agency, Office of General Counsel, 500 C Street, SW., Room 840, Washington, DC 20472 (for regional offices, consult your phone book).

K. Former components of the General Services Administration:

1. For the Federal Computer Incident Response Center and the Federal Protective Service: Chief, FOIA Information Management Branch, GSA (CAIM), 1800 F Street, NW., Washington, DC 20405 (for regional offices, consult your phone book).

### APPENDIX B TO PART 5 [RESERVED]

### APPENDIX C TO PART 5—DHS SYSTEMS OF RECORDS EXEMPT FROM THE PRIVACY ACT

This appendix implements provisions of the Privacy Act of 1974 that permit the Department of Homeland Security (DHS) to exempt its systems of records from provisions of the Act. During the course of normal agency operations, exempt materials from other systems of records may become part of the records in these and other DHS systems. To the extent that copies of records from other exempt systems of records are entered into any DHS system, DHS hereby claims the same exemptions for those records that are claimed for the original primary systems of records from which they originated and claims any additional exemptions in accordance with this rule.

Portions of the following DHS systems of records are exempt from certain provisions of the Privacy Act pursuant to 5 U.S.C. 552(j) and (k):

1. The DHS/ALL—001 Freedom of Information Act and Privacy Act Records System of Records consists of electronic and paper records and will be used by DHS and its components. The DHS/ALL—001 Freedom of Information Act and Privacy Act Records System of Records is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to the enforcement of civil and criminal laws; investigations, inquiries, and proceedings there under; national security and intelligence activities; and protection of the President of the United States or other individuals pursuant to section 3056 and 3056A of Title 18. The DHS/ALL—001 Freedom of Information Act and Privacy Act Records System of Records contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other federal, state, local, tribal, foreign, or international government agencies. The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to limitations set forth in 5 U.S.C. 552a(c)(3) and (4): (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8), (e)(12); (f); (g)(1); and (h) pursuant to 5 U.S.C. 552a(j)(2). Additionally, the Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to limitations set forth in 5 U.S.C. 552a(c)(3): (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f) pursuant to 5 U.S.C. §552a(k)(1), (k)(2), (k)(3), (k)(5), and (k)(6). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continually re-investigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced occasionally may be unclear, or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of the investigation, thereby interfering with that investigation and related law enforcement activities.

(e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information could impede law enforcement by compromising the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(f) From subsections (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements) and (f) (Agency Rules), because portions of this sys-

tem are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

(g) From subsection (e)(5) (Collection of Information) because with the collection of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with subsection (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.

(h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS's ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal and could result in disclosure of investigative techniques, procedures, and evidence.

(i) From subsection (e)(12) (Computer Matching) if the agency is a recipient agency or a source agency in a matching program with a non-Federal agency, with respect to any establishment or revision of a matching program, at least 30 days prior to conducting such program, publish in the FEDERAL REGISTER notice of such establishment or revision.

(j) From subsection (g)(1) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act.

(k) From subsection (h) (Legal Guardians) the parent of any minor, or the legal guardian of any individual who has been declared to be incompetent due to physical or mental incapacity or age by a court of competent jurisdiction, may act on behalf of the individual.

2. The DHS/ALL-029 Civil Rights and Civil Liberties Records System of Records consists of electronic and paper records and will be used by DHS and its components. The DHS/ALL-029 Civil Rights and Civil Liberties Records System of Records is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to the enforcement of civil and criminal laws; investigations, inquiries, and proceedings thereunder; national security and intelligence activities; and protection of the President of the United States or other individuals pursuant to Section 3056 and 3056A of Title 18. The DHS/ALL-029 Civil Rights and Civil Liberties

Records System of Records contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other Federal, state, local, Tribal, foreign, or international government agencies. The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to limitations set forth in 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f) pursuant to 5 U.S.C. §552a(k)(1), (k)(2), (k)(3), and (k)(5). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) (Accounting for Disclosures) because release of the accounting of disclosures could alert the individual who is the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would, therefore, present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the individual who is the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continually reinvestigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of Federal law, the accuracy of information obtained or introduced occasionally may be unclear, or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain

all information that may aid in establishing patterns of unlawful activity.

(d) From subsections (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements) and (f) (Agency Rules), because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

3. DHS–ALL–005, Redress and Response Records System. A portion of the following system of records is exempt from 5 U.S.C. 552a(c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (4)(G) through (I), (5), and (8); (f), and (g); however, these exemptions apply only to the extent that information in this system records is recompiled or is created from information contained in other systems of records subject to such exemptions pursuant to 5 U.S.C. 552a(j)(2), (k)(1), (k)(2), and (k)(5). Further, no exemption shall be asserted with respect to information submitted by and collected from the individual or the individual's representative in the course of any redress process associated with this system of records. After conferring with the appropriate component or agency, DHS may waive applicable exemptions in appropriate circumstances and where it would not appear to interfere with or adversely affect the law enforcement or national security purposes of the systems from which the information is recompiled or in which it is contained. Exemptions from the above particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, when information in this system records is recompiled or is created from information contained in other systems of records subject to exemptions for the following reasons:

(a) From subsection (c)(3) because making available to a record subject the accounting of disclosures from records concerning him or her would specifically reveal any investigative interest in the individual. Revealing this information could reasonably be expected to compromise ongoing efforts to investigate a known or suspected terrorist by notifying the record subject that he or she is under investigation. This information could also permit the record subject to take measures to impede the investigation, e.g., destroy evidence, intimidate potential witnesses, or flee the area to avoid or impede the investigation.

(b) From subsection (c)(4) because portions of this system are exempt from the access and amendment provisions of subsection (d).

(c) From subsections (d)(1), (2), (3), and (4) because these provisions concern individual access to and amendment of certain records contained in this system, including law enforcement counterterrorism, investigatory, and intelligence records. Compliance with these provisions could alert the subject of an investigation of the fact and nature of the investigation, and/or the investigative interest of intelligence or law enforcement agencies; compromise sensitive information related to national security; interfere with the overall law enforcement process by leading to the destruction of evidence, improper influencing of witnesses, fabrication of testimony, and/or flight of the subject; could identify a confidential source or disclose information which would constitute an unwarranted invasion of another's personal privacy; reveal a sensitive investigative or intelligence technique; or constitute a potential danger to the health or safety of law enforcement personnel, confidential informants, and witnesses. Amendment of these records would interfere with ongoing counterterrorism, law enforcement, or intelligence investigations and analysis activities and impose an impossible administrative burden by requiring investigations, analyses, and reports to be continuously reinvestigated and revised.

(d) From subsection (e)(1) because it is not always possible for DHS or other agencies to know in advance what information is relevant and necessary for it to complete an identity comparison between the individual seeking redress and a known or suspected terrorist. Also, because DHS and other agencies may not always know what information about an encounter with a known or suspected terrorist will be relevant to law enforcement for the purpose of conducting an operational response.

(e) From subsection (e)(2) because application of this provision could present a serious impediment to counterterrorism, law enforcement, or intelligence efforts in that it would put the subject of an investigation, study, or analysis on notice of that fact, thereby permitting the subject to engage in conduct designed to frustrate or impede that activity. The nature of counterterrorism, law enforcement, or intelligence investigations is such that vital information about an individual frequently can be obtained only from other persons who are familiar with such individual and his/her activities. In such investigations it is not feasible to rely upon information furnished by the individual concerning his own activities.

(f) From subsection (e)(3), to the extent that this subsection is interpreted to require DHS to provide notice to an individual if DHS or another agency receives or collects

information about that individual during an investigation or from a third party. Should the subsection be so interpreted, exemption from this provision is necessary to avoid impeding counterterrorism, law enforcement, or intelligence efforts by putting the subject of an investigation, study, or analysis on notice of that fact, thereby permitting the subject to engage in conduct intended to frustrate or impede that activity.

(g) From subsections (e)(4)(G), (H) and (I) (Agency Requirements) because portions of this system are exempt from the access and amendment provisions of subsection (d).

(h) From subsection (e)(5) because many of the records in this system coming from other system of records are derived from other domestic and foreign agency record systems and therefore it is not possible for DHS to vouch for their compliance with this provision; however, the DHS has implemented internal quality assurance procedures to ensure that data used in the redress process is as thorough, accurate, and current as possible. In addition, in the collection of information for law enforcement, counterterrorism, and intelligence purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light. The restrictions imposed by (e)(5) would limit the ability of those agencies' trained investigators and intelligence analysts to exercise their judgment in conducting investigations and impede the development of intelligence necessary for effective law enforcement and counterterrorism efforts. The DHS has, however, implemented internal quality assurance procedures to ensure that the data used in the redress process is as thorough, accurate, and current as possible.

(i) From subsection (e)(8) because to require individual notice of disclosure of information due to compulsory legal process would pose an impossible administrative burden on DHS and other agencies and could alert the subjects of counterterrorism, law enforcement, or intelligence investigations to the fact of those investigations when not previously known.

(j) From subsection (f) (Agency Rules) because portions of this system are exempt from the access and amendment provisions of subsection (d).

(k) From subsection (g) to the extent that the system is exempt from other specific subsections of the Privacy Act.

4. The Department of Homeland Security Automated Biometric Identification System (IDENT) consists of electronic and paper records and will be used by DHS and its components. IDENT is the primary repository of biometric information held by DHS in connection with its several and varied missions

and functions, including, but not limited to: The enforcement of civil and criminal laws (including the immigration law); investigations, inquiries, and proceedings thereunder; and national security and intelligence activities. IDENT is a centralized and dynamic DHS-wide biometric database that also contains limited biographic and encounter history information needed to place the biometric information in proper context. The information is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other Federal, State, local, tribal, foreign, or international government agencies.

Pursuant to exemptions 5 U.S.C. 552a(j)(2) of the Privacy Act, portions of this system are exempt from 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(5) and (e)(8); (f)(2) through (5); and (g). Pursuant to 5 U.S.C. 552a(k)(2), this system is exempt from the following provisions of the Privacy Act, subject to the limitations set forth in those subsections: 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), and (e)(4)(H). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation; and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, to the existence of the investigation, and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an impossible administrative burden by requiring investigations to be continuously re-investigated. In addition, permitting access and amendment to such information could

disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of Federal law, the accuracy of information obtained or introduced occasionally may be unclear or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of an investigation, thereby interfering with the related investigation and law enforcement activities.

(e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information would impede law enforcement in that it could compromise the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(f) From subsections (e)(4)(G) and (H) (Agency Requirements), and (f)(2) through (5) (Agency Rules) because portions of this system are exempt from the individual access provisions of subsection (d) and thereby would not require DHS to establish requirements or rules for records which are exempted from access.

(g) From subsection (e)(5) (Collection of Information) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.

(h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS' ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal, and could result in disclosure of investigative techniques, procedures, and evidence.

(i) From subsection (g) to the extent that the system is exempt from other specific subsections of the Privacy Act.

5. The DHS/OIG-002 Investigative Records System of Records consists of electronic and paper records used by the DHS OIG. The DHS/OIG-002 Investigative Records System of Records is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to the enforcement of civil and criminal laws; investigations, inquiries, and proceedings there under; and national security and intelligence activities. The

DHS/OIG-002 Investigative Records System of Records contains information that is collected by, on behalf of, in support of, or in cooperation with DHS components and may contain personally identifiable information collected by other federal, state, local, tribal, foreign, or international government agencies. The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to limitations set forth in 5 U.S.C. 552a(c)(3) and (c)(4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(5) and (e)(8); (f); and (g) pursuant to 5 U.S.C. 552a(j)(2). Additionally, the Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to limitations set forth in 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H); and (f) pursuant to 5 U.S.C. 552a(k)(1), (k)(2) and (k)(5). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (c)(4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, to the existence of the investigation; and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, tamper with witnesses or evidence, and avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, to the existence of the investigation, and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, tamper with witnesses or evidence, and avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an impossible administrative burden by requiring investigations to be continuously reinvestigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of federal law, the accuracy of informa-

tion obtained or introduced occasionally may be unclear or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject as to the nature or existence of an investigation, thereby interfering with the related investigation and law enforcement activities.

(e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information would impede law enforcement in that it could compromise investigations by: revealing the existence of an otherwise confidential investigation and thereby providing an opportunity for the subject of an investigation to conceal evidence, alter patterns of behavior, or take other actions that could thwart investigative efforts; revealing the identity of witnesses in investigations thereby providing an opportunity for the subjects of the investigations or others to harass, intimidate, or otherwise interfere with the collection of evidence or other information from such witnesses; or revealing the identity of confidential informants, which would negatively affect the informants' usefulness in any ongoing or future investigations and discourage members of the public from cooperating as confidential informants in any future investigations.

(f) From subsections (e)(4)(G) and (e)(4)(H) (Agency Requirements) and (f) (Agency Rules), because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish rules or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in this system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, potential witnesses, and confidential informants.

(g) From subsection (e)(5) (Collection of Information) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.

(h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS' ability to obtain, serve, and issue

subpoenas, warrants and other law enforcement mechanisms that may be filed under seal, and could result in disclosure of investigative techniques, procedures, and evidence.

(i) From subsection (g) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act relating to individuals' rights to access and amend their records contained in the system. Therefore, DHS is not required to establish rules or procedures pursuant to which individuals may seek a civil remedy for the agency's refusals to amend a record; refusal to comply with a request for access to records; failure to maintain accurate, relevant, timely, and complete records; or failure to otherwise comply with an individual's right to access or amend records.

6. The Immigration and Customs Enforcement (ICE) Pattern Analysis and Information Collection (ICEPIC) System consists of electronic and paper records and will be used by DHS and its components. ICEPIC is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to: The enforcement of civil and criminal laws (including the immigration law); investigations, inquiries, and proceedings there under; and national security and intelligence activities. ICEPIC contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other Federal, State, local, tribal, foreign, or international government agencies.

Pursuant to exemption 5 U.S.C. 552a(j)(2) of the Privacy Act, portions of this system are exempt from 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(5) and (e)(8); (f), and (g). Pursuant to 5 U.S.C. 552a(k)(2), this system is exempt from the following provisions of the Privacy Act, subject to the limitations set forth in those subsections: 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), and (f). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation, and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence,

and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, to the existence of the investigation, and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an impossible administrative burden by requiring investigations to be continuously re-investigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of Federal law, the accuracy of information obtained or introduced occasionally may be unclear or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of an investigation, thereby interfering with the related investigation and law enforcement activities.

(e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information would impede law enforcement in that it could compromise investigations by: revealing the existence of an otherwise confidential investigation and thereby provide an opportunity for the subject of an investigation to conceal evidence, alter patterns of behavior, or take other actions that could thwart investigative efforts; reveal the identity of witnesses in investigations, thereby providing an opportunity for the subjects of the investigations or others to harass, intimidate, or otherwise interfere with the collection of evidence or other information from such witnesses; or reveal the identity of confidential informants, which would negatively affect the informant's usefulness in any ongoing or future investigations and discourage members of the public from cooperating as confidential informants in any future investigations.

(f) From subsections (e)(4)(G) and (H) (Agency Requirements), and (f) (Agency

Rules) because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

(g) From subsection (e)(5) (Collection of Information) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.

(h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS' ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal, and could result in disclosure of investigative techniques, procedures, and evidence.

(i) From subsection (g) to the extent that the system is exempt from other specific subsections of the Privacy Act relating to individuals' rights to access and amend their records contained in the system. Therefore DHS is not required to establish rules or procedures pursuant to which individuals may seek a civil remedy for the agency's: Refusal to amend a record; Refusal to comply with a request for access to records; failure to maintain accurate, relevant timely and complete records; or failure to otherwise comply with an individual's right to access or amend records.

7. The Office of Intelligence and Analysis (I&A) Enterprise Records System (ERS) consists of records including intelligence information and other properly acquired information received from agencies and components of the federal government, foreign governments, organizations or entities, international organizations, state and local government agencies (including law enforcement agencies), and private sector entities, as well as information provided by individuals, regardless of the medium used to submit the information or the agency to which it was submitted. This system also contains: Information regarding persons on watch lists with known or suspected links to terrorism; the results of intelligence analysis and reporting; ongoing law enforcement investigative information, information systems security analysis and reporting; active immigra-

tion, customs, border and transportation, security related records; historical law enforcement, operational, immigration, customs, border and transportation security, and other administrative records; relevant and appropriately acquired financial information; and public-source data such as that contained in media reports and commercially available databases, as appropriate. Data about the providers of information, including the means of transmission of the data, is also retained.

(a) Pursuant to 5 U.S.C. 552a(k)(1), (2), (3), and (5), this system of records is exempt from 5 U.S.C. 552a(c)(3), (d)(1), (2), (3), (4), and (5), (e)(1), (e)(4)(G), (H), and (I), and (f). These exemptions apply only to the extent that information in this system is subject to exemption. Where compliance would not appear to interfere with or adversely affect the intelligence, counterterrorism, homeland security, and related law enforcement purposes of this system, the applicable exemption may be waived by DHS.

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) (Accounting for Disclosures) because making available to a record subject the accounting of disclosures from records concerning him/her would specifically reveal any interest in the individual of an intelligence, counterterrorism, homeland security, or related investigative nature. Revealing this information could reasonably be expected to compromise ongoing efforts of the Department to identify, understand, analyze, investigate, and counter the activities of:

(i) Known or suspected terrorists and terrorist groups;

(ii) Groups or individuals known or believed to be assisting or associated with known or suspected terrorists or terrorist groups;

(iii) Individuals known, believed to be, or suspected of being engaged in activities constituting a threat to homeland security, including (1) activities which impact or concern the security, safety, and integrity of our international borders, including any illegal activities that either cross our borders or are otherwise in violation of the immigration or customs laws and regulations of the United States; (2) activities which could reasonably be expected to assist in the development or use of a weapon of mass effect; (3) activities meant to identify, create, or exploit the vulnerabilities of, or undermine, the "key resources" (as defined in section 2(9) of the Homeland Security Act of 2002) and "critical infrastructure" (as defined in 42 U.S.C. 5195c(c)) of the United States, including the cyber and national telecommunications infrastructure and the availability of a viable national security and emergency

preparedness communications infrastructure; (4) activities detrimental to the security of transportation and transportation systems; (5) activities which violate or are suspected of violating the laws relating to counterfeiting of obligations and securities of the United States and other financial crimes, including access device fraud, financial institution fraud, identity theft, computer fraud; and computer-based attacks on our nation's financial, banking, and telecommunications infrastructure; (6) activities, not wholly conducted within the United States, which violate or are suspected of violating the laws which prohibit the production, transfer, or sale of narcotics or substances controlled in accordance with Title 21 of the United States Code, or those associated activities otherwise prohibited by Titles 21 and 46 of the United States Code; (7) activities which impact, concern, or otherwise threaten the safety and security of the President and Vice President, their families, heads of state, and other designated individuals; the White House, Vice President's residence, foreign missions, and other designated buildings within the United States; (8) activities which impact, concern, or otherwise threaten domestic maritime safety and security, maritime mobility and navigation, or the integrity of the domestic maritime environment; (9) activities which impact, concern, or otherwise threaten the national operational capability of the Department to respond to natural and manmade major disasters and emergencies, including acts of terrorism; (10) activities involving the importation, possession, storage, development, or transportation of nuclear or radiological material without authorization or for use against the United States;

(iv) Foreign governments, organizations, or persons (foreign powers); and

(v) Individuals engaging in intelligence activities on behalf of a foreign power or terrorist group.

Thus, by notifying the record subject that he/she is the focus of such efforts or interest on the part of DHS, or other agencies with whom DHS is cooperating and to whom the disclosures were made, this information could permit the record subject to take measures to impede or evade such efforts, including the taking of steps to deceive DHS personnel and deny them the ability to adequately assess relevant information and activities, and could inappropriately disclose to the record subject the sensitive methods and/or confidential sources used to acquire the relevant information against him/her. Moreover, where the record subject is the actual target of a law enforcement investigation, this information could permit him/her to take measures to impede the investigation, for example, by destroying evidence, intimidating potential witnesses, or avoiding detection or apprehension.

(2) From subsections (d)(1), (2), (3), and (4) (Access to Records) because these provisions concern individual rights of access to and amendment of records (including the review of agency denials of either) contained in this system, which consists of intelligence, counterterrorism, homeland security, and related investigatory records concerning efforts of the Department, as described more fully in subsection (b)(1), above. Compliance with these provisions could inform or alert the subject of an intelligence, counterterrorism, homeland security, or investigatory effort undertaken on behalf of the Department, or by another agency with whom DHS is cooperating, of the fact and nature of such efforts, and/or the relevant intelligence, counterterrorism, homeland security, or investigatory interest of DHS and/or other intelligence, counterterrorism, or law enforcement agencies. Moreover, compliance could also compromise sensitive information either classified in the interest of national security, or which otherwise requires, as appropriate, safeguarding and protection from unauthorized disclosure; identify a confidential source or disclose information which would constitute an unwarranted invasion of another individual's personal privacy; reveal a sensitive intelligence or investigative technique or method, including interfering with intelligence or law enforcement investigative processes by permitting the destruction of evidence, improper influencing or intimidation of witnesses, fabrication of statements or testimony, and flight from detection or apprehension; or constitute a potential danger to the health or safety of intelligence, counterterrorism, homeland security, and law enforcement personnel, confidential sources and informants, and potential witnesses. Amendment of the records would interfere with ongoing intelligence, counterterrorism, homeland security, and law enforcement investigations and activities, including incident reporting and analysis activities, and impose an impossible administrative burden by requiring investigations, reports, and analyses to be continuously reinvestigated and revised.

(3) From subsection (e)(1) (Relevant and Necessary) because it is not always possible for DHS to know in advance of its receipt the relevance and necessity of each piece of information it acquires in the course of an intelligence, counterterrorism, or investigatory effort undertaken on behalf of the Department, or by another agency with whom DHS is cooperating. In the context of the authorized intelligence, counterterrorism, and investigatory activities undertaken by DHS personnel, relevance and necessity are questions of analytic judgment and timing, such that what may appear relevant and necessary when acquired ultimately may be deemed unnecessary upon further analysis

and evaluation. Similarly, in some situations, it is only after acquired information is collated, analyzed, and evaluated in light of other available evidence and information that its relevance and necessity can be established or made clear. Constraining the initial acquisition of information included within the ERS in accordance with the relevant and necessary requirement of subsection (e)(1) could discourage the appropriate receipt of and access to information which DHS and I&A are otherwise authorized to receive and possess under law, and thereby impede efforts to detect, deter, prevent, disrupt, or apprehend terrorists or terrorist groups, and/or respond to terrorist or other activities which threaten homeland security. Notwithstanding this claimed exemption, which would permit the acquisition and temporary maintenance of records whose relevance to the purpose of the ERS may be less than fully clear, DHS will only disclose such records after determining whether such disclosures are themselves consistent with the published ERS routine uses. Moreover, it should be noted that, as concerns the receipt by I&A, for intelligence purposes, of information in any record which identifies a U.S. Person, as defined in Executive Order 12333, as amended, such receipt, and any subsequent use or dissemination of that identifying information, is undertaken consistent with the procedures established and adhered to by I&A pursuant to that Executive Order. Specifically, I&A intelligence personnel may acquire information which identifies a particular U.S. Person, retain it within or disseminate it from ERS, as appropriate, only when it is determined that the personally identifying information is necessary for the conduct of I&A's functions, and otherwise falls into one of a limited number of authorized categories, each of which reflects discrete activities for which information on individuals would be utilized by the Department in the overall execution of its statutory mission.

(4) From subsections (e)(4) (G), (H) and (I) (Access), and (f) (Agency Rules), inasmuch as it is unnecessary for the publication of rules and procedures contemplated therein since the ERS, pursuant to subsections (1) and (2), above, will be exempt from the underlying duties to provide to individuals notification about, access to, and the ability to amend or correct the information pertaining to them in, this system of records. Furthermore, to the extent that subsection (e)(4)(I) is construed to require more detailed disclosure than the information accompanying the system notice for ERS, as published in today's FEDERAL REGISTER, exemption from it is also necessary to protect the confidentiality, privacy, and physical safety of sources of information, as well as the methods for acquiring it. Finally, greater specificity concerning the description of categories of sources of

properly classified records could also compromise or otherwise cause damage to the national or homeland security.

8. The information in MAGNET establishes Maritime Domain Awareness. Maritime Domain Awareness is the collection of as much information as possible about the maritime world. In other words, MAGNET establishes a full awareness of the entities (people, places, things) and their activities within the maritime industry. MAGNET collects the information and connects the information in order to fulfill this need.

Coast Guard Intelligence (through MAGNET) will provide awareness to the field as well as to strategic planners by aggregating data from existing sources internal and external to the Coast Guard or DHS. MAGNET will correlate and provide the medium to display information such as ship registry, current ship position, crew background, passenger lists, port history, cargo, known criminal vessels, and suspect lists. Coast Guard Intelligence (CG-2) will serve as MAGNET's executive agent and will share appropriate aggregated data to other law enforcement and intelligence agencies.

(a) Pursuant to 5 U.S.C. 522a(j)(2), (k)(1), and (k)(2) this system of records is exempt from 5 U.S.C. 552a(c)(3) and (4), (d)(1), (d)(2), (d)(3), (d)(4), (e)(1), (e)(2), (e)(3), (e)(4) (G), (H), and (I), e(5), e(8), e(12), (f), and (g). These exemptions apply only to the extent that information in this system is subject to exemption. Where compliance would not appear to interfere with or adversely affect the intelligence, counterterrorism, homeland security, and related law enforcement purposes of this system, the applicable exemption may be waived by DHS.

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) (Accounting of Certain Disclosures) because making available to a record subject the accounting of disclosures from records concerning him/her would specifically reveal any interest in the individual of an intelligence, counterterrorism, homeland security, law enforcement or related investigative nature. Revealing this information could reasonably be expected to compromise ongoing efforts of the Department to identify, understand, analyze, investigate, and counter the activities of:

(i) Known or suspected terrorists and terrorist groups;

(ii) Groups or individuals known or believed to be assisting or associated with known or suspected terrorists or terrorist groups;

(iii) Individuals known, believed to be, or suspected of being engaged in activities constituting a threat to homeland security, including (1) activities which impact or concern the security, safety, and integrity of

our international borders, including any illegal activities that either cross our borders or are otherwise in violation of the immigration or customs laws and regulations of the United States; (2) activities which could reasonably be expected to assist in the development or use of a weapon of mass effect; (3) activities meant to identify, create, or exploit the vulnerabilities of, or undermine, the “key resources” (as defined in section 2(9) of the Homeland Security Act of 2002) and “critical infrastructure” (as defined in 42 U.S.C. 5195c(c)) of the United States, including the cyber and national telecommunications infrastructure and the availability of a viable national security and emergency preparedness communications infrastructure; (4) activities detrimental to the security of transportation and transportation systems; (5) activities which violate or are suspected of violating the laws relating to counterfeiting of obligations and securities of the United States and other financial crimes, including access device fraud, financial institution fraud, identity theft, computer fraud; and computer-based attacks on our nation’s financial, banking, and telecommunications infrastructure; (6) activities, not wholly conducted within the United States, which violate or are suspected of violating the laws which prohibit the production, transfer, or sale of narcotics or substances controlled in accordance with Title 21 of the United States Code, or those associated activities otherwise prohibited by Titles 21 and 46 of the United States Code; (7) activities which impact, concern, or otherwise threaten the safety and security of the President and Vice President, their families, heads of state, and other designated individuals; the White House, Vice President’s residence, foreign missions, and other designated buildings within the United States; (8) activities which impact, concern, or otherwise threaten domestic maritime safety and security, maritime mobility and navigation, or the integrity of the domestic maritime environment; (9) activities which impact, concern, or otherwise threaten the national operational capability of the Department to respond to natural and manmade major disasters and emergencies, including acts of terrorism; (10) activities involving the importation, possession, storage, development, or transportation of nuclear or radiological material without authorization or for use against the United States;

(iv) Foreign governments, organizations, or persons (foreign powers); and

(v) Individuals engaging in intelligence activities on behalf of a foreign power or terrorist group.

Thus, by notifying the record subject that he/she is the focus of such efforts or interest on the part of DHS, or other agencies with whom DHS is cooperating and to whom the disclosures were made, this information

could permit the record subject to take measures to impede or evade such efforts, including the taking of steps to deceive DHS personnel and deny them the ability to adequately assess relevant information and activities, and could inappropriately disclose to the record subject the sensitive methods and/or confidential sources used to acquire the relevant information against him/her. Moreover, where the record subject is the actual target of a law enforcement investigation, this information could permit him/her to take measures to impede the investigation, for example, by destroying evidence, intimidating potential witnesses, or avoiding detection or apprehension.

(2) From subsection (c)(4) (Accounting for Disclosure, notice of dispute) because certain records in this system are exempt from the access and amendment provisions of subsection (d), this requirement to inform any person or other agency about any correction or notation of dispute that the agency made with regard to those records, should not apply.

(3) From subsections (d)(1), (2), (3), and (4) (Access to Records) because these provisions concern individual rights of access to and amendment of records (including the review of agency denials of either) contained in this system, which consists of intelligence, counterterrorism, homeland security, and related investigatory records concerning efforts of the Department, as described more fully in subsection (b)(1), above. Compliance with these provisions could inform or alert the subject of an intelligence, counterterrorism, homeland security, or investigatory effort undertaken on behalf of the Department, or by another agency with whom DHS is cooperating, of the fact and nature of such efforts, and/or the relevant intelligence, counterterrorism, homeland security, or investigatory interest of DHS and/or other intelligence, counterterrorism, or law enforcement agencies. Moreover, compliance could also compromise sensitive information either classified in the interest of national security, or which otherwise requires, as appropriate, safeguarding and protection from unauthorized disclosure; identify a confidential source or disclose information which would constitute an unwarranted invasion of another individual’s personal privacy; reveal a sensitive intelligence or investigative technique or method, including interfering with intelligence or law enforcement investigative processes by permitting the destruction of evidence, improper influencing or intimidation of witnesses, fabrication of statements or testimony, and flight from detection or apprehension; or constitute a potential danger to the health or safety of intelligence, counterterrorism, homeland security, and law enforcement personnel, confidential sources and informants, and potential witnesses. Amendment of the records

would interfere with ongoing intelligence, counterterrorism, homeland security, and law enforcement investigations and activities, including incident reporting and analysis activities, and impose an impossible administrative burden by requiring investigations, reports, and analyses to be continuously reinvestigated and revised.

(4) From subsection (e)(1) (Relevant and Necessary) because it is not always possible for DHS to know in advance of its receipt the relevance and necessity of each piece of information it acquires in the course of an intelligence, counterterrorism, or investigatory effort undertaken on behalf of the Department, or by another agency with whom DHS is cooperating. In the context of the authorized intelligence, counterterrorism, and investigatory activities undertaken by DHS personnel, relevance and necessity are questions of analytic judgment and timing, such that what may appear relevant and necessary when acquired ultimately may be deemed unnecessary upon further analysis and evaluation. Similarly, in some situations, it is only after acquired information is collated, analyzed, and evaluated in light of other available evidence and information that its relevance and necessity can be established or made clear. Constraining the initial acquisition of information included within the MAGNET in accordance with the relevant and necessary requirement of subsection (e)(1) could discourage the appropriate receipt of and access to information which DHS and MAGNET are otherwise authorized to receive and possess under law, and thereby impede efforts to detect, deter, prevent, disrupt, or apprehend terrorists or terrorist groups, and/or respond to terrorist or other activities which threaten homeland security. Notwithstanding this claimed exemption, which would permit the acquisition and temporary maintenance of records whose relevance to the purpose of the MAGNET may be less than fully clear, DHS will only disclose such records after determining whether such disclosures are themselves consistent with the published MAGNET routine uses. Moreover, it should be noted that, as concerns the receipt by USCG, for intelligence purposes, of information in any record which identifies a U.S. Person, as defined in Executive Order 12333, as amended, such receipt, and any subsequent use or dissemination of that identifying information, is undertaken consistent with the procedures established and adhered to by USCG pursuant to that Executive Order. Specifically, USCG intelligence personnel may acquire information which identifies a particular U.S. Person, retain it within or disseminate it from MAGNET, as appropriate, only when it is determined that the personally identifying information is necessary for the conduct of USCG's functions, and otherwise falls into one of a limited number of authorized cat-

egories, each of which reflects discrete activities for which information on individuals would be utilized by the Department in the overall execution of its statutory mission.

(5) From subsection (e)(2) (Collection of Information from Individuals) because application of this provision could present a serious impediment to counterterrorism or law enforcement efforts in that it would put the subject of an investigation, study or analysis on notice of that fact, thereby permitting the subject to engage in conduct designed to frustrate or impede that activity. The nature of counterterrorism and law enforcement investigations is such that vital information about an individual frequently can be obtained only from other persons who are familiar with such individual and his/her activities. In such investigations it is not feasible to rely solely upon information furnished by the individual concerning his own activities.

(6) From subsection (e)(3) (Notice to Subjects), to the extent that this subsection is interpreted to require DHS to provide notice to an individual if DHS or another agency receives or collects information about that individual during an investigation or from a third party. Should the subsection be so interpreted, exemption from this provision is necessary to avoid impeding counterterrorism or law enforcement efforts by putting the subject of an investigation, study or analysis on notice of that fact, thereby permitting the subject to engage in conduct intended to frustrate or impede that activity.

(7) From subsections (e)(4) (G), (H) and (I) (Access), and (f) (Agency Rules), inasmuch as it is unnecessary for the publication of rules and procedures contemplated therein since the MAGNET, pursuant to subsections (3), above, will be exempt from the underlying duties to provide to individuals notification about, access to, and the ability to amend or correct the information pertaining to them in, this system of records. Furthermore, to the extent that subsection (e)(4)(I) is construed to require more detailed disclosure than the information accompanying the system notice for MAGNET, as published in today's FEDERAL REGISTER, exemption from it is also necessary to protect the confidentiality, privacy, and physical safety of sources of information, as well as the methods for acquiring it. Finally, greater specificity concerning the description of categories of sources of properly classified records could also compromise or otherwise cause damage to the national or homeland security.

(8) From subsection (e)(5) (Collection of Information) because many of the records in this system coming from other system of records are derived from other domestic and foreign agency record systems and therefore it is not possible for DHS to vouch for their compliance with this provision; however, the

DHS has implemented internal quality assurance procedures to ensure that data used in its screening processes is as complete, accurate, and current as possible. In addition, in the collection of information for law enforcement and counterterrorism purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light. The restrictions imposed by (e)(5) would limit the ability of those agencies' trained investigators and intelligence analysts to exercise their judgment in conducting investigations and impede the development of intelligence necessary for effective law enforcement and counterterrorism efforts.

(9) From subsection (e)(8) (Notice on Individuals) because to require individual notice of disclosure of information due to compulsory legal process would pose an impossible administrative burden on DHS and other agencies and could alert the subjects of counterterrorism or law enforcement investigations to the fact of those investigations then not previously known.

(10) From subsection (e)(12) (Matching Agreements) because requiring DHS to provide notice of alterations to existing matching agreements would impair DHS operations by indicating which data elements and information are valuable to DHS's analytical functions, thereby providing harmful disclosure of information to individuals who would seek to circumvent or interfere with DHS's missions.

(11) From subsection (g) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act.

9. The Law Enforcement Information Data Base (LEIDB)/Pathfinder is a historical repository of selected Coast Guard message traffic. LEIDB/Pathfinder supports law enforcement intelligence activities. LEIDB/Pathfinder users can query archived message traffic and link relevant information across multiple data records within LEIDB/Pathfinder. Users have system tools enabling the user to identify potential relationships between information contained in otherwise unrelated documents. These tools allow the analysts to build high precision and low return queries, which minimize false hits and maximize analyst productivity while working with unstructured, unformatted, free test documents.

(a) Pursuant to 5 U.S.C. 552a(j)(2), (k)(1), and (k)(2) certain records or information in the above mentioned system of records are exempt from 5 U.S.C. 552a(c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (4)(G) through (I), (e)(5), and (8); (f), and (g). These exemptions apply only to the extent that information in this system is subject to exemption. Where compliance would not appear to inter-

fere with or adversely affect the intelligence, counterterrorism, homeland security, and related law enforcement purposes of this system, the applicable exemption may be waived by DHS.

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) (Accounting for Disclosures) because making available to a record subject the accounting of disclosures from records concerning him/her would specifically reveal any interest in the individual of an intelligence, counterterrorism, homeland security, or related investigative nature. Revealing this information could reasonably be expected to compromise ongoing efforts of the Department to identify, understand, analyze, investigate, and counter the activities of:

(i) Known or suspected terrorists and terrorist groups;

(ii) Groups or individuals known or believed to be assisting or associated with known or suspected terrorists or terrorist groups;

(iii) Individuals known, believed to be, or suspected of being engaged in activities constituting a threat to homeland security, including (1) activities which impact or concern the security, safety, and integrity of our international borders, including any illegal activities that either cross our borders or are otherwise in violation of the immigration or customs laws and regulations of the United States; (2) activities which could reasonably be expected to assist in the development or use of a weapon of mass effect; (3) activities meant to identify, create, or exploit the vulnerabilities of, or undermine, the "key resources" (as defined in section 2(9) of the Homeland Security Act of 2002) and "critical infrastructure" (as defined in 42 U.S.C. 5195c(c)) of the United States, including the cyber and national telecommunications infrastructure and the availability of a viable national security and emergency preparedness communications infrastructure; (4) activities detrimental to the security of transportation and transportation systems; (5) activities which violate or are suspected of violating the laws relating to counterfeiting of obligations and securities of the United States and other financial crimes, including access device fraud, financial institution fraud, identity theft, computer fraud; and computer-based attacks on our nation's financial, banking, and telecommunications infrastructure; (6) activities, not wholly conducted within the United States, which violate or are suspected of violating the laws which prohibit the production, transfer, or sale of narcotics or substances controlled in accordance with Title 21 of the United States Code, or those associated activities otherwise prohibited by Titles 21 and 46 of the United States Code; (7)

activities which impact, concern, or otherwise threaten the safety and security of the President and Vice President, their families, heads of state, and other designated individuals; the White House, Vice President's residence, foreign missions, and other designated buildings within the United States; (8) activities which impact, concern, or otherwise threaten domestic maritime safety and security, maritime mobility and navigation, or the integrity of the domestic maritime environment; (9) activities which impact, concern, or otherwise threaten the national operational capability of the Department to respond to natural and manmade major disasters and emergencies, including acts of terrorism; (10) activities involving the importation, possession, storage, development, or transportation of nuclear or radiological material without authorization or for use against the United States;

(iv) Foreign governments, organizations, or persons (foreign powers); and

(v) Individuals engaging in intelligence activities on behalf of a foreign power or terrorist group.

Thus, by notifying the record subject that he/she is the focus of such efforts or interest on the part of DHS, or other agencies with whom DHS is cooperating and to whom the disclosures were made, this information could permit the record subject to take measures to impede or evade such efforts, including the taking of steps to deceive DHS personnel and deny them the ability to adequately assess relevant information and activities, and could inappropriately disclose to the record subject the sensitive methods and/or confidential sources used to acquire the relevant information against him/her. Moreover, where the record subject is the actual target of a law enforcement investigation, this information could permit him/her to take measures to impede the investigation, for example, by destroying evidence, intimidating potential witnesses, or avoiding detection or apprehension.

(2) From subsection (c)(4) (Accounting for Disclosure, notice of dispute) because certain records in this system are exempt from the access and amendment provisions of subsection (d), this requirement to inform any person or other agency about any correction or notation of dispute that the agency made with regard to those records, should not apply.

(3) From subsections (d)(1), (2), (3), and (4) (Access to Records) because these provisions concern individual rights of access to and amendment of records (including the review of agency denials of either) contained in this system, which consists of intelligence, counterterrorism, homeland security, and related investigatory records concerning efforts of the Department, as described more fully in subsection (b)(1), above. Compliance with these provisions could inform or alert

the subject of an intelligence, counterterrorism, homeland security, or investigatory effort undertaken on behalf of the Department, or by another agency with whom DHS is cooperating, of the fact and nature of such efforts, and/or the relevant intelligence, counterterrorism, homeland security, or investigatory interest of DHS and/or other intelligence, counterterrorism, or law enforcement agencies. Moreover, compliance could also compromise sensitive information either classified in the interest of national security, or which otherwise requires, as appropriate, safeguarding and protection from unauthorized disclosure; identify a confidential source or disclose information which would constitute an unwarranted invasion of another individual's personal privacy; reveal a sensitive intelligence or investigative technique or method, including interfering with intelligence or law enforcement investigative processes by permitting the destruction of evidence, improper influencing or intimidation of witnesses, fabrication of statements or testimony, and flight from detection or apprehension; or constitute a potential danger to the health or safety of intelligence, counterterrorism, homeland security, and law enforcement personnel, confidential sources and informants, and potential witnesses. Amendment of the records would interfere with ongoing intelligence, counterterrorism, homeland security, and law enforcement investigations and activities, including incident reporting and analysis activities, and impose an impossible administrative burden by requiring investigations, reports, and analyses to be continuously reinvestigated and revised.

(4) From subsection (e)(1) (Relevant and Necessary) because it is not always possible for DHS to know in advance of its receipt the relevance and necessity of each piece of information it acquires in the course of an intelligence, counterterrorism, or investigatory effort undertaken on behalf of the Department, or by another agency with whom DHS is cooperating. In the context of the authorized intelligence, counterterrorism, and investigatory activities undertaken by DHS personnel, relevance and necessity are questions of analytic judgment and timing, such that what may appear relevant and necessary when acquired ultimately may be deemed unnecessary upon further analysis and evaluation. Similarly, in some situations, it is only after acquired information is collated, analyzed, and evaluated in light of other available evidence and information that its relevance and necessity can be established or made clear. Constraining the initial acquisition of information included within the LEIDB in accordance with the relevant and necessary requirement of subsection (e)(1) could discourage the appropriate receipt of and access to information

which DHS and USCG are otherwise authorized to receive and possess under law, and thereby impede efforts to detect, deter, prevent, disrupt, or apprehend terrorists or terrorist groups, and/or respond to terrorist or other activities which threaten homeland security. Notwithstanding this claimed exemption, which would permit the acquisition and temporary maintenance of records whose relevance to the purpose of the LEIDB may be less than fully clear, DHS will only disclose such records after determining whether such disclosures are themselves consistent with the published LEIDB routine uses. Moreover, it should be noted that, as concerns the receipt by USCG, for intelligence purposes, of information in any record which identifies a U.S. Person, as defined in Executive Order 12333, as amended, such receipt, and any subsequent use or dissemination of that identifying information, is undertaken consistent with the procedures established and adhered to by USCG pursuant to that Executive Order. Specifically, USCG intelligence personnel may acquire information which identifies a particular U.S. Person, retain it within or disseminate it from LEIDB, as appropriate, only when it is determined that the personally identifying information is necessary for the conduct of USCG's functions, and otherwise falls into one of a limited number of authorized categories, each of which reflects discrete activities for which information on individuals would be utilized by the Department in the overall execution of its statutory mission.

(5) From subsection (e)(2) (Collection of Information from Individuals) because application of this provision could present a serious impediment to counterterrorism or law enforcement efforts in that it would put the subject of an investigation, study or analysis on notice of that fact, thereby permitting the subject to engage in conduct designed to frustrate or impede that activity. The nature of counterterrorism, and law enforcement investigations is such that vital information about an individual frequently can be obtained only from other persons who are familiar with such individual and his/her activities. In such investigations it is not feasible to rely solely upon information furnished by the individual concerning his own activities.

(6) From subsection (e)(3) (Notice to Subjects), to the extent that this subsection is interpreted to require DHS to provide notice to an individual if DHS or another agency receives or collects information about that individual during an investigation or from a third party. Should the subsection be so interpreted, exemption from this provision is necessary to avoid impeding counterterrorism or law enforcement efforts by putting the subject of an investigation, study or analysis on notice of that fact, thereby per-

mitting the subject to engage in conduct intended to frustrate or impede that activity.

(7) From subsections (e)(4) (G), (H) and (I) (Access), inasmuch as it is unnecessary for the publication of rules and procedures contemplated therein since the LEIDB, pursuant to subsections (2) and (3), above, will be exempt from the underlying duties to provide to individuals notification about, access to, and the ability to amend or correct the information pertaining to them in, this system of records. Furthermore, to the extent that subsection (e)(4)(I) is construed to require more detailed disclosure than the information accompanying the system notice for LEIDB, as published in today's FEDERAL REGISTER, exemption from it is also necessary to protect the confidentiality, privacy, and physical safety of sources of information, as well as the methods for acquiring it. Finally, greater specificity concerning the description of categories of sources of properly classified records could also compromise or otherwise cause damage to the national or homeland security.

(8) From subsection (e)(5) (Collection of Information) because many of the records contained in this system are derived from other domestic and foreign sources, it is not possible for DHS to vouch for those records' compliance with this provision; however, the DHS has implemented internal quality assurance procedures to ensure that data used in its screening processes is as complete, accurate, and current as possible. In addition, in the collection of information for law enforcement and counterterrorism purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light. The restrictions imposed by (e)(5) would limit the ability of those agencies' trained investigators and intelligence analysts to exercise their judgment in conducting investigations and impede the development of intelligence necessary for effective law enforcement and counterterrorism efforts.

(9) From subsection (e)(8) (Notice on Individuals) because to require individual notice of disclosure of information due to compulsory legal process would pose an impossible administrative burden on DHS and other agencies and could alert the subjects of counterterrorism or law enforcement investigations to the fact of those investigations then not previously known.

(10) From subsection (f) (Agency Rules) because portions of this system are exempt from the access and amendment provisions of subsection (d). Access to, and amendment of, system records that are not exempt or for which exemption is waived may be obtained under procedures described in the related SORN or subpart B of this part.

(11) From subsection (g) to the extent that the system is exempt from other specific subsections of the Privacy Act relating to individuals' rights to access and amend their records contained in the system. Therefore DHS is not required to establish rules or procedures pursuant to which individuals may seek a civil remedy for the agency's: Refusal to amend a record; refusal to comply with a request for access to records; failure to maintain accurate, relevant timely and complete records; or failure to otherwise comply with an individual's right to access or amend records.

10. DHS-ICE-001, The Immigration and Customs Enforcement (ICE) Student and Exchange Visitor Information System (SEVIS) collects and maintains pertinent information on nonimmigrant students and exchange visitors and the schools and exchange visitor program sponsors that host them while in the United States. The system permits DHS to monitor compliance by these individuals with the terms of their admission into the United States. Pursuant to exemptions (j)(2), (k)(1), (k)(2) and (k)(5) of the Privacy Act, portions of this system are exempt from 5 U.S.C. 552a(c)(3); (d); (e)(1); (e)(4)(G), (H) and (I). Exemptions from the particular subsections are justified, on a case by case basis, to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation, of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation and avoid detection or apprehension, which undermines the entire system.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation, of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation and avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and impose an impossible administrative burden by requiring investigations to be continuously reinvestigated. In addition, permitting access and amendment to such information also could

disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced occasionally may be unclear or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective enforcement of federal laws, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsections (e)(4)(G), (H) and (I) (Agency Requirements), and (f) (Agency Rules), because portions of this system are exempt from the access provisions of subsection (d).

11. The General Counsel Electronic Management System (GEMS) consists of records and information created or collected by attorneys for U.S. Immigration and Customs Enforcement, which will be used in the preparation and presentation of cases before a court or other adjudicative body. ICE attorneys work closely with ICE law enforcement personnel throughout the process of adjudicating immigration cases. GEMS allows ICE attorneys to store all the materials pertaining to immigration adjudications, including documents related to investigations, case notes and other hearing related information, and briefs and memoranda of law related to cases. Having this information in one system should not only facilitate the work of the ICE attorneys involved in the particular case, but also will provide a legal resource for other attorneys who are adjudicating similar cases. The system will also provide management capabilities for tracking time and effort expended in the preparation and presentation of cases. Pursuant to exemptions 5 U.S.C. 552a(j)(2) of the Privacy Act, portions of this system are exempt from 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(5) and (e)(8); (f)(2) through (5); and (g). Pursuant to 5 U.S.C. 552a (k)(1) and (k)(2), this system is exempt from the following provisions of the Privacy Act, subject to the limitations set forth in those subsections: 5 U.S.C. 552a (c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), and (f). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, to the existence of the investigation, which in some cases may be classified, and reveal investigative interest on the part of DHS or ICE. Disclosure of the accounting would therefore present a serious impediment to

law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, tamper with witnesses or evidence, and avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation pertaining to an immigration matter, which in some cases may be classified, and prematurely reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, tamper with witnesses or evidence, and avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an impossible administrative burden by requiring investigations to be continuously reinvestigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of federal immigration law, the accuracy of information obtained or introduced occasionally may be unclear or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement and for the protection of national security, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject of the nature or existence of an investigation, which could cause interference with the investigation, a related inquiry or other law enforcement activities, some of which may be classified.

(e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information would impede law enforcement in that it could compromise the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(f) From subsections (e)(4)(G) and (H) (Agency Requirements), (f) (Agency Rules), and (g) (Civil Remedies) because portions of this system are exempt from the individual access provisions of subsection (d).

(g) From subsection (e)(5) (Collection of Information) because in the collection of information for law enforcement purposes it is impossible to determine in advance what in-

formation is accurate, relevant, timely, and complete.

(h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with ICE's ability to obtain, serve, and issue subpoenas, warrants and other law enforcement mechanisms that may be filed under seal, and could result in disclosure of investigative techniques, procedures, and evidence.

(i) From subsection (g) to the extent that the system is exempt from other specific subsections of the Privacy Act.

12. DHS/CBP-005, Advanced Passenger Information System. A portion of the following system of records is exempt from 5 U.S.C. 552a(c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (4)(G) through (I), (5), and (8); (f), and (g); however, these exemptions apply only to the extent that information in this system records is recompiled or is created from information contained in other systems of records subject to such exemptions pursuant to 5 U.S.C. 552a(j)(2), and (k)(2). Further, no exemption shall be asserted with respect to information submitted by and collected from the individual or the individual's representative in the course of any redress process associated with this system of records. After conferring with the appropriate component or agency, DHS may waive applicable exemptions in appropriate circumstances and where it would not appear to interfere with or adversely affect the law enforcement or national security purposes of the systems from which the information is recompiled or in which it is contained. Exemptions from the above particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, when information in this system records is recompiled or is created from information contained in other systems of records subject to exemptions for the following reasons:

(a) From subsection (c)(3) (Accounting for Disclosure) because making available to a record subject the accounting of disclosures from records concerning him or her would specifically reveal any investigative interest in the individual. Revealing this information could reasonably be expected to compromise ongoing efforts to investigate a known or suspected terrorist by notifying the record subject that he or she is under investigation. This information could also permit the record subject to take measures to impede the investigation, e.g., destroy evidence, intimidate potential witnesses, or flee the area to avoid or impede the investigation.

(b) From subsection (c)(4) (Accounting for Disclosure, notice of dispute) because portions of this system are exempt from the access and amendment provisions of subsection (d).

(c) From subsections (d)(1), (2), (3), and (4) (Access to Records) because these provisions concern individual access to and amendment

of certain records contained in this system, including law enforcement counterterrorism, investigatory, and intelligence records. Compliance with these provisions could alert the subject of an investigation of the fact and nature of the investigation, and/or the investigative interest of intelligence or law enforcement agencies; compromise sensitive information related to national security; interfere with the overall law enforcement process by leading to the destruction of evidence, improper influencing of witnesses, fabrication of testimony, and/or flight of the subject; could identify a confidential source or disclose information which would constitute an unwarranted invasion of another's personal privacy; reveal a sensitive investigative or intelligence technique; or constitute a potential danger to the health or safety of law enforcement personnel, confidential informants, and witnesses. Amendment of these records would interfere with ongoing counterterrorism, law enforcement, or intelligence investigations and analysis activities and impose an impossible administrative burden by requiring investigations, analyses, and reports to be continuously re-investigated and revised.

(d) From subsection (e)(1) (Relevancy and Necessity of Information) because it is not always possible for DHS or other agencies to know in advance what information is relevant and necessary for it to complete an identity comparison between the individual seeking redress and a known or suspected terrorist. Also, because DHS and other agencies may not always know what information about an encounter with a known or suspected terrorist will be relevant to law enforcement for the purpose of conducting an operational response.

(e) From subsection (e)(2) (Collection of Information from Individuals) because application of this provision could present a serious impediment to counterterrorism, law enforcement, or intelligence efforts in that it would put the subject of an investigation, study, or analysis on notice of that fact, thereby permitting the subject to engage in conduct designed to frustrate or impede that activity. The nature of counterterrorism, law enforcement, or intelligence investigations is such that vital information about an individual frequently can be obtained only from other persons who are familiar with such individual and his/her activities. In such investigations it is not feasible to rely upon information furnished by the individual concerning his own activities.

(f) From subsection (e)(3) (Notice to Subjects), to the extent that this subsection is interpreted to require DHS to provide notice to an individual if DHS or another agency receives or collects information about that individual during an investigation or from a third party. Should the subsection be so interpreted, exemption from this provision is

necessary to avoid impeding counterterrorism, law enforcement, or intelligence efforts by putting the subject of an investigation, study, or analysis on notice of that fact, thereby permitting the subject to engage in conduct intended to frustrate or impede that activity.

(g) From subsections (e)(4)(G), (H) and (I) (Agency Requirements) because portions of this system are exempt from the access and amendment provisions of subsection (d).

(h) From subsection (e)(5) (Collection of Information) because many of the records in this system coming from other system of records are derived from other domestic and foreign agency record systems and therefore it is not possible for DHS to vouch for their compliance with this provision; however, the DHS has implemented internal quality assurance procedures to ensure that data used in the redress process is as thorough, accurate, and current as possible. In addition, in the collection of information for law enforcement, counterterrorism, and intelligence purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light. The restrictions imposed by (e)(5) would limit the ability of those agencies' trained investigators and intelligence analysts to exercise their judgment in conducting investigations and impede the development of intelligence necessary for effective law enforcement and counterterrorism efforts. The DHS has, however, implemented internal quality assurance procedures to ensure that the data used in the redress process is as thorough, accurate, and current as possible.

(i) From subsection (e)(8) (Notice on Individuals) because to require individual notice of disclosure of information due to compulsory legal process would pose an impossible administrative burden on DHS and other agencies and could alert the subjects of counterterrorism, law enforcement, or intelligence investigations to the fact of those investigations when not previously known.

(j) From subsection (f) (Agency Rules) because portions of this system are exempt from the access and amendment provisions of subsection (d).

(k) From subsection (g) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act.

13. The Department of Homeland Security General Training Records system of records consists of electronic and paper records and will be used by DHS and its components. The Department of Homeland Security General Training Records system of records consists of electronic and paper records and will be used by DHS and its components and offices

to maintain records about individual training, including enrollment and participation information, information pertaining to class schedules, programs, and instructors, training trends and needs, testing and examination materials, and assessments of training efficacy. The data will be collected by employee name or other unique identifier. The collection and maintenance of this information will assist DHS in meeting its obligation to train its personnel and contractors in order to ensure that the agency mission can be successfully accomplished. Pursuant to exemptions 5 U.S.C. 552a(k)(6) of the Privacy Act, portions of this system are exempt from 5 U.S.C. 552a(d) to the extent that records in this system relate to testing or examination materials used solely to determine individual qualifications for appointment in the Federal service. Access to or amendment of this information by the data subject would compromise the objectivity and fairness of the testing and examination process.

14. The U.S. ICE-005 Trade Transparency Analysis and Research (TTAR) System consists of electronic and paper records and will be used by the Department of Homeland Security (DHS). TTAR is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to: The enforcement of civil and criminal laws; investigations, inquiries, and proceedings there under; and national security and intelligence activities. TTAR contains information that is collected by other federal and foreign government agencies and may contain personally identifiable information. Pursuant to exemption 5 U.S.C. 552a(j)(2) of the Privacy Act, portions of this system are exempt from 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(5) and (e)(8); (f), and (g). Pursuant to 5 U.S.C. 552a(k)(2), this system is exempt from the following provisions of the Privacy Act, subject to the limitations set forth in those subsections: 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), and (f). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation, and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension,

which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, to the existence of the investigation, and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an impossible administrative burden by requiring investigations to be continuously re-investigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of Federal law, the accuracy of information obtained or introduced occasionally may be unclear or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of an investigation, thereby interfering with the related investigation and law enforcement activities.

(e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information would impede law enforcement in that it could compromise investigations by: Revealing the existence of an otherwise confidential investigation and thereby provide an opportunity for the subject of an investigation to conceal evidence, alter patterns of behavior, or take other actions that could thwart investigative efforts; reveal the identity of witnesses in investigations, thereby providing an opportunity for the subjects of the investigations or others to harass, intimidate, or otherwise interfere with the collection of evidence or other information from such witnesses; or reveal the identity of confidential informants, which would negatively affect the informant's usefulness in any ongoing or future investigations and discourage members of the public from cooperating as confidential informants in any future investigations.

(f) From subsections (e)(4)(G) and (H) (Agency Requirements), and (f) (Agency Rules) because portions of this system are

exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, potential witnesses, and confidential informants.

(g) From subsection (e)(5) (Collection of Information) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.

(h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS's ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal, and could result in disclosure of investigative techniques, procedures, and evidence.

(i) From subsection (g) to the extent that the system is exempt from other specific subsections of the Privacy Act relating to individuals' rights to access and amend their records contained in the system. Therefore DHS is not required to establish rules or procedures pursuant to which individuals may seek a civil remedy for the agency's: Refusal to amend a record; refusal to comply with a request for access to records; failure to maintain accurate, relevant, timely and complete records; or failure to otherwise comply with an individual's right to access or amend records.

15. The DHS/ALL—013 Claims Records system of records consists of electronic and paper records and will be used by DHS and its components. The DHS/ALL—013 Claims Records system is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to: the enforcement of civil and criminal laws; investigations, inquiries, and proceedings there under; and national security, intelligence activities; and protection of the President of the United States or other individuals pursuant to section 3056 and 3056A of Title 18. The DHS/ALL—013 Claims Records system contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other Federal, State, local, Tribal, foreign, or international government agencies. The

Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to limitations set forth in 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5) and (e)(8); (f), and (g) pursuant to 5 U.S.C. 552a(j)(2). Additionally, the Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to limitations set forth in 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (I), and (f) pursuant to 5 U.S.C. 552a(k)(1), (k)(2), and (k)(3). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation, and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, to the existence of the investigation, and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an impossible administrative burden by requiring investigations to be continuously re-investigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of Federal law, the accuracy of information obtained or introduced occasionally may be unclear or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of an investigation, thereby interfering with the related investigation and law enforcement activities.

(e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information would impede law enforcement in that it could compromise investigations by: revealing the existence of an otherwise confidential investigation and thereby provide an opportunity for the subject of an investigation to conceal evidence, alter patterns of behavior, or take other actions that could thwart investigative efforts; reveal the identity of witnesses in investigations, thereby providing an opportunity for the subjects of the investigations or others to harass, intimidate, or otherwise interfere with the collection of evidence or other information from such witnesses; or reveal the identity of confidential informants, which would negatively affect the informant's usefulness in any ongoing or future investigations and discourage members of the public from cooperating as confidential informants in any future investigations.

(f) From subsections (e)(4)(G), (H), and (I) (Agency Requirements), and (f) (Agency Rules) because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

(g) From subsection (e)(5) (Collection of Information) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.

(h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS' ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal, and could result in disclosure of investigative techniques, procedures, and evidence.

(i) From subsection (g) to the extent that the system is exempt from other specific

subsections of the Privacy Act relating to individuals' rights to access and amend their records contained in the system. Therefore DHS is not required to establish rules or procedures pursuant to which individuals may seek a civil remedy for the agency's: refusal to amend a record; refusal to comply with a request for access to records; failure to maintain accurate, relevant timely and complete records; or failure to otherwise comply with an individual's right to access or amend records.

16. [Reserved]

17. The DHS/ALL—006 Accident Records system of records consists of electronic and paper records and will be used by DHS and its components. The DHS/ALL—006 Accident Records system is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to: the enforcement of civil and criminal laws; investigations, inquiries, and proceedings thereunder; national security and intelligence activities; and protection of the President of the United States or other individuals pursuant to section 3056 and 3056A of Title 18. The DHS/ALL—006 Accident Records system contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other Federal, State, local, tribal, foreign, or international government agencies. The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(d) pursuant to 5 U.S.C. 552a(k)(3). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons: From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of information related to the protection of a President of the United States or other individuals pursuant to section 3056 and 3056A of Title 18. Permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

18. The DHS/ALL—020 Internal Affairs Records system of records consists of electronic and paper records and will be used by DHS and its components. The DHS/ALL—020 Internal Affairs Records system is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to: The enforcement of civil and criminal laws; investigations, inquiries, and proceedings thereunder; national security and intelligence activities; and protection of the President of the United States or other individuals pursuant to section 3056 and 3056A of Title 18. The DHS/ALL—020 Internal Affairs

Records system contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other Federal, State, local, tribal, foreign, or international government agencies. The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5) and (e)(8); (f), and (g) pursuant to 5 U.S.C. 552a(j)(2). Additionally, the Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a (c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f) pursuant to 5 U.S.C. 552a(k)(1), (k)(2), (k)(3), and (k)(5). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation, and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, to the existence of the investigation, and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an impossible administrative burden by requiring investigations to be continuously re-investigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of Federal law, the accuracy of infor-

mation obtained or introduced occasionally may be unclear or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of an investigation, thereby interfering with the related investigation and law enforcement activities.

(e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information would impede law enforcement in that it could compromise investigations by: revealing the existence of an otherwise confidential investigation and thereby provide an opportunity for the subject of an investigation to conceal evidence, alter patterns of behavior, or take other actions that could thwart investigative efforts; reveal the identity of witnesses in investigations, thereby providing an opportunity for the subjects of the investigations or others to harass, intimidate, or otherwise interfere with the collection of evidence or other information from such witnesses; or reveal the identity of confidential informants, which would negatively affect the informant's usefulness in any ongoing or future investigations and discourage members of the public from cooperating as confidential informants in any future investigations.

(f) From subsections (e)(4)(G), (H), and (I) (Agency Requirements), and (f) (Agency Rules) because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

(g) From subsection (e)(5) (Collection of Information) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with (e)(5) would preclude DHS agents from using their investigative training, and exercise of good judgment to both conduct and report on investigations.

(h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS' ability to obtain, serve, and issue

subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal, and could result in disclosure of investigative techniques, procedures, and evidence.

(i) From subsection (g) to the extent that the system is exempt from other specific subsections of the Privacy Act relating to individuals' rights to access and amend their records contained in the system. Therefore DHS is not required to establish rules or procedures pursuant to which individuals may seek a civil remedy for the agency's: refusal to amend a record; refusal to comply with a request for access to records; failure to maintain accurate, relevant timely and complete records; or failure to otherwise comply with an individual's right to access or amend records.

19. The DHS/ALL—024 Facility and Perimeter Access Control and Visitor Management system of records consists of electronic and paper records and will be used by DHS and its components. The DHS/ALL—024 Facility and Perimeter Access Control and Visitor Management system is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to: the enforcement of civil and criminal laws; investigations, inquiries, and proceedings there under; and national security and intelligence activities. The DHS/ALL—024 Facility and Perimeter Access Control and Visitor Management system contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other Federal, State, local, tribal, foreign, or international government agencies. The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a (c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f) pursuant to 5 U.S.C. 552a(k)(1), (k)(2), and (k)(5). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation, and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid

detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, to the existence of the investigation, and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an impossible administrative burden by requiring investigations to be continuously re-investigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of Federal law, the accuracy of information obtained or introduced occasionally may be unclear or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsections (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements), and (f) (Agency Rules) because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

20. The DHS/CBP—009 Electronic System for Travel Authorization system of records consists of electronic and paper records and will be used by DHS and its Components. The DHS/CBP—009 Electronic System for Travel Authorization system is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to: The enforcement of civil and criminal laws; investigations, inquiries, and proceedings thereunder; and national security and intelligence activities. The DHS/CBP—009 Electronic System for Travel Authorization system contains information that is collected

by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other Federal, State, local, tribal, foreign, or international government agencies. The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(c)(3), (e)(8), and (g) pursuant to 5 U.S.C. 552a(j)(2), and (k)(2). Further, no exemption shall be asserted with respect to information maintained in the system as it relates to data submitted by or on behalf of a person who travels to visit the United States and crosses the border, nor shall an exemption be asserted with respect to the resulting determination (approval or denial). After conferring with the appropriate component or agency, DHS may waive applicable exemptions in appropriate circumstances and where it would not appear to interfere with or adversely affect the law enforcement purposes of the systems from which the information is recompiled or in which it is contained. Exemptions from the above particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, when information in this system of records may impede a law enforcement or national security investigation:

(a) From subsection (c)(3) (Accounting for Disclosure) because making available to a record subject the accounting of disclosures from records concerning him or her would specifically reveal any investigative interest in the individual. Revealing this information could reasonably be expected to compromise ongoing efforts to investigate a violation of U.S. law, including investigations of a known or suspected terrorist, by notifying the record subject that he or she is under investigation. This information could also permit the record subject to take measures to impede the investigation, e.g., destroy evidence, intimidate potential witnesses, or flee the area to avoid or impede the investigation.

(b) From subsection (e)(8) (Notice on Individuals) because to require individual notice of disclosure of information due to compulsory legal process would pose an impossible administrative burden on DHS and other agencies and could alert the subjects of counterterrorism or law enforcement investigations to the fact of those investigations when not previously known.

(c) From subsection (g) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act.

21. The DHS/CBP—010 Persons Engaged in International Trade in CBP Licensed/Regulated Activities system of records consists of electronic and paper records and will be used by DHS and its components. The DHS/CBP—010 Persons Engaged in International Trade in CBP Licensed/Regulated Activities is a re-

pository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to: The enforcement of civil and criminal laws; investigations, inquiries, and proceedings thereunder; and national security and intelligence activities. The DHS/CBP—010 Persons Engaged in International Trade in CBP Licensed/Regulated Activities contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other Federal, State, local, tribal, foreign, or international government agencies. The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5) and (e)(8); (f), and (g) pursuant to 5 U.S.C. 552a(j)(2). Additionally, the Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a (c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f) pursuant to 5 U.S.C. 552a(k)(2). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation, and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, to the existence of the investigation, and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an

impossible administrative burden by requiring investigations to be continuously re-investigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to national security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of Federal law, the accuracy of information obtained or introduced occasionally may be unclear or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of an investigation, thereby interfering with the related investigation and law enforcement activities.

(e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information would impede law enforcement in that it could compromise investigations by: Revealing the existence of an otherwise confidential investigation and thereby provide an opportunity for the subject of an investigation to conceal evidence, alter patterns of behavior, or take other actions that could thwart investigative efforts; reveal the identity of witnesses in investigations, thereby providing an opportunity for the subjects of the investigations or others to harass, intimidate, or otherwise interfere with the collection of evidence or other information from such witnesses; or reveal the identity of confidential informants, which would negatively affect the informant's usefulness in any ongoing or future investigations and discourage members of the public from cooperating as confidential informants in any future investigations.

(f) From subsections (e)(4)(G), (H), and (I) (Agency Requirements), and (f) (Agency Rules) because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

(g) From subsection (e)(5) (Collection of Information) because in the collection of information for law enforcement purposes it is

impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.

(h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS' ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal, and could result in disclosure of investigative techniques, procedures, and evidence.

(i) From subsection (g) to the extent that the system is exempt from other specific subsections of the Privacy Act relating to individuals' rights to access and amend their records contained in the system. Therefore DHS is not required to establish rules or procedures pursuant to which individuals may seek a civil remedy for the agency's: Refusal to amend a record; refusal to comply with a request for access to records; failure to maintain accurate, relevant, timely and complete records; or failure to otherwise comply with an individual's right to access or amend records.

22. The DHS/CBP—011 TECS system of records consists of electronic and paper records and will be used by DHS, its Components, and other Federal agencies. The DHS/CBP—011 TECS is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to: The enforcement of civil and criminal laws; investigations, inquiries, and proceedings thereunder; and national security and intelligence activities. The DHS/CBP—011 TECS contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other Federal, State, local, Tribal, foreign, or international government agencies. The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5) and (e)(8); (f), and (g) pursuant to 5 U.S.C. 552a(j)(2). Additionally, the Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a (c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f) pursuant to 5 U.S.C. 552a(k)(2). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the

accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation, and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, to the existence of the investigation, and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an impossible administrative burden by requiring investigations to be continuously re-investigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to national security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of Federal law, the accuracy of information obtained or introduced occasionally may be unclear or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation or subject of interest would alert the subject to the nature or existence of an investigation, thereby interfering with the related investigation and law enforcement activities or national security matter.

(e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information would impede law enforcement in that it could compromise investigations by: Revealing the existence of an otherwise confidential investigation and thereby provide an opportunity for the subject of an investigation to conceal evidence, alter patterns of behavior, or take other actions that could thwart investigative efforts; reveal the iden-

tity of witnesses in investigations, thereby providing an opportunity for the subjects of the investigations or others to harass, intimidate, or otherwise interfere with the collection of evidence or other information from such witnesses; or reveal the identity of confidential informants, which would negatively affect the informant's usefulness in any ongoing or future investigations and discourage members of the public from cooperating as confidential informants in any future investigations.

(f) From subsections (e)(4)(G), (H), and (I) (Agency Requirements), and (f) (Agency Rules) because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

(g) From subsection (e)(5) (Collection of Information) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.

(h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS' ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal, and could result in disclosure of investigative techniques, procedures, and evidence.

(i) From subsection (g) to the extent that the system is exempt from other specific subsections of the Privacy Act relating to individuals' rights to access and amend their records contained in the system. Therefore DHS is not required to establish rules or procedures pursuant to which individuals may seek a civil remedy for the agency's: Refusal to amend a record; refusal to comply with a request for access to records; failure to maintain accurate, relevant, timely and complete records; or failure to otherwise comply with an individual's right to access or amend records.

23. The DHS/CBP—012 Closed Circuit Tele- vision system of records consists of elec- tronic and paper records and will be used by DHS and its components. The DHS/CBP—012

Closed Circuit Television system is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to: The enforcement of civil and criminal laws; investigations, inquiries, and proceedings thereunder; and national security and intelligence activities. The DHS/CBP–012 Closed Circuit Television system contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other Federal, State, local, tribal, foreign, or international government agencies. The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(c)(3) and (4): (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5) and (e)(8); (f), and (g) pursuant to 5 U.S.C. 552a(j)(2). Additionally, the Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f) pursuant to 5 U.S.C. 552a(k)(2). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation, and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, to the existence of the investigation, and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an impossible administrative burden by requiring investigations to be continuously re-

investigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of Federal law, the accuracy of information obtained or introduced occasionally may be unclear or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of an investigation, thereby interfering with the related investigation and law enforcement activities.

(e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information would impede law enforcement in that it could compromise investigations by: Revealing the existence of an otherwise confidential investigation and thereby provide an opportunity for the subject of an investigation to conceal evidence, alter patterns of behavior, or take other actions that could thwart investigative efforts; reveal the identity of witnesses in investigations, thereby providing an opportunity for the subjects of the investigations or others to harass, intimidate, or otherwise interfere with the collection of evidence or other information from such witnesses; or reveal the identity of confidential informants, which would negatively affect the informant's usefulness in any ongoing or future investigations and discourage members of the public from cooperating as confidential informants in any future investigations.

(f) From subsections (e)(4)(G), (H), and (I) (Agency Requirements), and (f) (Agency Rules) because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

(g) From subsection (e)(5) (Collection of Information) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and

complete. Compliance with (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.

(h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS' ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal, and could result in disclosure of investigative techniques, procedures, and evidence.

(i) From subsection (g) to the extent that the system is exempt from other specific subsections of the Privacy Act relating to individuals' rights to access and amend their records contained in the system. Therefore DHS is not required to establish rules or procedures pursuant to which individuals may seek a civil remedy for the agency's: Refusal to amend a record; refusal to comply with a request for access to records; failure to maintain accurate, relevant, timely and complete records; or failure to otherwise comply with an individual's right to access or amend records.

24. The DHS/CBP—013 Seized Assets and Case Tracking System (SEACATS) consists of electronic and paper records and will be used by DHS and its components. The DHS/CBP—013 Seized Assets and Case Tracking System is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to: The enforcement of civil and criminal laws; investigations, inquiries, and proceedings thereunder; and national security and intelligence activities. The DHS/CBP—013 Seized Assets and Case Tracking System contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other Federal, State, local, tribal, foreign, or international government agencies. The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5) and (e)(8); (f), and (g) pursuant to 5 U.S.C. 552a(j)(2). Additionally, the Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a (c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (I), and (f) pursuant to 5 U.S.C. 552a(k)(2). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or po-

tential criminal, civil, or regulatory violation to the existence of the investigation, and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, to the existence of the investigation, and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an impossible administrative burden by requiring investigations to be continuously re-investigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to national security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of Federal law, the accuracy of information obtained or introduced occasionally may be unclear or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of an investigation, thereby interfering with the related investigation and law enforcement activities.

(e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information would impede law enforcement in that it could compromise investigations by: Revealing the existence of an otherwise confidential investigation and thereby provide an opportunity for the subject of an investigation to conceal evidence, alter patterns of behavior, or take other actions that could thwart investigative efforts; reveal the identity of witnesses in investigations, thereby providing an opportunity for the subjects of

the investigations or others to harass, intimidate, or otherwise interfere with the collection of evidence or other information from such witnesses; or reveal the identity of confidential informants, which would negatively affect the informant's usefulness in any ongoing or future investigations and discourage members of the public from cooperating as confidential informants in any future investigations.

(f) From subsections (e)(4)(G), (H), and (I) (Agency Requirements), and (f) (Agency Rules) because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

(g) From subsection (e)(5) (Collection of Information) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with (e)(5) would preclude the officers and agents of DHS components' from using their investigative training and exercise of good judgment to both conduct and report on investigations.

(h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS' ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal, and could result in disclosure of investigative techniques, procedures, and evidence.

(i) From subsection (g) to the extent that the system is exempt from other specific subsections of the Privacy Act relating to individuals' rights to access and amend their records contained in the system. Therefore DHS is not required to establish rules or procedures pursuant to which individuals may seek a civil remedy for the agency's: Refusal to amend a record; refusal to comply with a request for access to records; failure to maintain accurate, relevant timely and complete records; or failure to otherwise comply with an individual's right to access or amend records.

25. The Department of Homeland Security (DHS)/U.S. Customs and Border Protection-014 Regulatory Audit Archive System (RAAS) System of Records consists of electronic and paper records and will be used by DHS and its Components. The DHS/CBP-014 RAAS System of Records is a repository of information held by DHS in connection with

its several and varied missions and functions, including, but not limited to: the enforcement of civil and criminal laws; investigations; inquiries; and proceedings there under. The DHS/CBP-014 RAAS System of Records contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its Components and may contain personally identifiable information collected by other Federal, State, local, tribal, foreign, or international government agencies. The Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(k)(2), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, to the existence of the investigation, and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an impossible administrative burden by requiring investigations to be continuously re-investigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of Federal law, the accuracy of information obtained or introduced occasionally may be unclear or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain

all information that may aid in establishing patterns of unlawful activity.

(d) From subsections (e)(4)(G), (H), and (I) (Agency Requirements), and (f) (Agency Rules) because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

26. DHS/CBP-001, Import Information System (IIS). A portion of the following system of records is exempt from 5 U.S.C. 552a(c)(3), (e)(8), and (g)(1) pursuant to 5 U.S.C. 552a(j)(2), and from 5 U.S.C. 552a(c)(3) pursuant to 5 U.S.C. 552a(k)(2). Further, no exemption shall be asserted with respect to information maintained in the system as it relates to data submitted by or on behalf of a person who travels to visit the United States and crosses the border, nor shall an exemption be asserted with respect to the resulting determination (approval or denial). After conferring with the appropriate component or agency, DHS may waive applicable exemptions in appropriate circumstances and where it would not appear to interfere with or adversely affect the law enforcement purposes of the systems from which the information is recompiled or in which it is contained. Exemptions from the above particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, when information in this system of records is may impede a law enforcement, intelligence activities and national security investigation:

(a) From subsection (c)(3) (Accounting for Disclosure) because making available to a record subject the accounting of disclosures from records concerning him or her would specifically reveal any investigative interest in the individual. Revealing this information could reasonably be expected to compromise ongoing efforts to investigate a violation of U.S. law, including investigations of a known or suspected terrorist, by notifying the record subject that he or she is under investigation. This information could also permit the record subject to take measures to impede the investigation, *e.g.*, destroy evidence, intimidate potential witnesses, or flee the area to avoid or impede the investigation.

(b) From subsection (e)(8) (Notice on Individuals) because to require individual notice of disclosure of information due to compulsory legal process would pose an impossible

administrative burden on DHS and other agencies and could alert the subjects of counterterrorism or law enforcement investigations to the fact of those investigations when not previously known.

(c) From subsection (g)(1) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act.

27. The DHS/CBP-009 Nonimmigrant Information system of records consists of electronic and paper records and will be used by DHS and its Components. The DHS/CBP-009 Nonimmigrant Information System is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to: The enforcement of civil and criminal laws; Investigations, inquiries, and proceedings thereunder; and national security and intelligence activities. The DHS/CBP-009 Nonimmigrant Information System contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other Federal, State, local, Tribal, foreign, or international government agencies. This system may contain records or information pertaining to the accounting of disclosures made from the Nonimmigrant Information System to other law enforcement and counterterrorism agencies (Federal, State, Local, Foreign, International or Tribal) in accordance with the published routine uses. The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 522(c)(3), (e) (8), and (g) of the Privacy Act of 1974, as amended, as necessary and appropriate to protect accounting of these disclosures only, pursuant to 5 U.S.C. 552a (j)(2), and (k)(2). Further, no exemption shall be asserted with respect to biographical or travel information submitted by, and collected from, a person's travel documents or submitted from a government computer system to support or to validate those travel documents. After conferring with the appropriate component or agency, DHS may waive applicable exemptions in appropriate circumstances and where it would not appear to interfere with or adversely affect the law enforcement purposes of the systems from which the information is recompiled or in which it is contained. Exemptions from the above particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, when information in this system of records is recompiled or is created from information contained in other systems of records subject to exemptions for the following reasons:

(a) From subsection (c)(3) (Accounting for Disclosure) because making available to a record subject the accounting of disclosures from records concerning him or her would

specifically reveal any investigative interest in the individual. Revealing this information could reasonably be expected to compromise ongoing efforts to investigate a violation of U.S. law, including investigations of a known or suspected terrorist, by notifying the record subject that he or she is under investigation. This information could also permit the record subject to take measures to impede the investigation, e.g., destroy evidence, intimidate potential witnesses, or flee the area to avoid or impede the investigation.

(b) From subsection (e)(8) (Notice on Individuals) because to require individual notice of disclosure of information due to compulsory legal process would pose an impossible administrative burden on DHS and other agencies and could alert the subjects of counterterrorism or law enforcement investigations to the fact of those investigations when not previously known.

(c) From subsection (g) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act.

28. The DHS/ICE—007 Law Enforcement Support Center (LESC) Alien Criminal Response Information Management (ACRIME) system of records consists of electronic and paper records and will be used by DHS and its components. The DHS/ICE—007 Law Enforcement Support Center Alien Criminal Response Information Management system is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to: The enforcement of civil and criminal laws; investigations, inquiries, and proceedings thereunder; and national security and intelligence activities. The DHS/ICE—007 Law Enforcement Support Center Alien Criminal Response Information Management system contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other Federal, State, local, tribal, foreign, or international government agencies. The Secretary of Homeland Security has exempted this system of records from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), and (e)(5) and (e)(8); (f), and (g) pursuant to 5 U.S.C. 552a(j)(2). Additionally, the Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a (c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), and (f) pursuant to 5 U.S.C. 552a(k)(2). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the

accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation, and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, to the existence of the investigation, and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an impossible administrative burden by requiring investigations to be continuously re-investigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of Federal law, the accuracy of information obtained or introduced occasionally may be unclear or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in identifying or establishing patterns of unlawful activity.

(d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of an investigation, thereby interfering with the related investigation and law enforcement activities.

(e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information would impede law enforcement in that it could compromise investigations by: Revealing the existence of an otherwise confidential investigation and thereby provide an opportunity for the subject of an investigation to conceal evidence, alter patterns of behavior, or take other actions that could thwart investigative efforts; reveal the identity of witnesses in investigations, thereby

providing an opportunity for the subjects of the investigations or others to harass, intimidate, or otherwise interfere with the collection of evidence or other information from such witnesses; or reveal the identity of confidential informants, which would negatively affect the informant's usefulness in any ongoing or future investigations and discourage members of the public from cooperating as confidential informants in any future investigations.

(f) From subsections (e)(4)(G), (H) (Agency Requirements), and (f) (Agency Rules) because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

(g) From subsection (e)(5) (Collection of Information) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.

(h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS' ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal, and could result in disclosure of investigative techniques, procedures, and evidence.

(i) From subsection (g) to the extent that the system is exempt from other specific subsections of the Privacy Act relating to individuals' rights to access and amend their records contained in the system. Therefore DHS is not required to establish rules or procedures pursuant to which individuals may seek a civil remedy for the agency's: Refusal to amend a record; refusal to comply with a request for access to records; failure to maintain accurate, relevant, timely and complete records; or failure to otherwise comply with an individual's right to access or amend records.

29. The DHS/ICE—008 Search, Arrest, and Seizure system of records consists of electronic and paper records and will be used by DHS and its components. The DHS/ICE—008 Search, Arrest, and Seizure system is a repository of information held by DHS in connection with its several and varied missions

and functions, including, but not limited to: The enforcement of civil and criminal laws; investigations, inquiries, and proceedings thereunder; and national security and intelligence activities. The DHS/ICE—008 Search, Arrest, and Seizure system contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other Federal, State, local, tribal, foreign, or international government agencies. The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(5) and (e)(8); (f), and (g) pursuant to 5 U.S.C. 552a(j)(2). Additionally, the Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), and (f) pursuant to 5 U.S.C. 552a(k)(2). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation, and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, to the existence of the investigation, and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an impossible administrative burden by requiring investigations to be continuously re-investigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of Federal law, the accuracy of information obtained or introduced occasionally may be unclear or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of an investigation, thereby interfering with the related investigation and law enforcement activities.

(e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information would impede law enforcement in that it could compromise investigations by: Revealing the existence of an otherwise confidential investigation and thereby provide an opportunity for the subject of an investigation to conceal evidence, alter patterns of behavior, or take other actions that could thwart investigative efforts; reveal the identity of witnesses in investigations, thereby providing an opportunity for the subjects of the investigations or others to harass, intimidate, or otherwise interfere with the collection of evidence or other information from such witnesses; or reveal the identity of confidential informants, which would negatively affect the informant's usefulness in any ongoing or future investigations and discourage members of the public from cooperating as confidential informants in any future investigations.

(f) From subsections (e)(4)(G) and (H) (Agency Requirements), and (f) (Agency Rules) because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

(g) From subsection (e)(5) (Collection of Information) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment

to both conduct and report on investigations.

(h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS' ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal, and could result in disclosure of investigative techniques, procedures, and evidence.

(i) From subsection (g) to the extent that the system is exempt from other specific subsections of the Privacy Act relating to individuals' rights to access and amend their records contained in the system. Therefore DHS is not required to establish rules or procedures pursuant to which individuals may seek a civil remedy for the agency's: Refusal to amend a record; refusal to comply with a request for access to records; failure to maintain accurate, relevant, timely and complete records; or failure to otherwise comply with an individual's right to access or amend records.

30. The DHS/ICE—009 External Investigations system of records consists of electronic and paper records and will be used by DHS and its components. The DHS/ICE—009 External Investigations system is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to: The enforcement of civil and criminal laws; investigations, inquiries, and proceedings there under; and national security and intelligence activities. The DHS/ICE—009 External Investigations system contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other Federal, State, local, tribal, foreign, or international government agencies. The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), and (e)(5) and (e)(8); (f), and (g) pursuant to 5 U.S.C. 552a(j)(2). Additionally, the Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), and (f) pursuant to 5 U.S.C. 552a(k)(2). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation, and reveal investigative interest on the part

of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, to the existence of the investigation, and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an impossible administrative burden by requiring investigations to be continuously re-investigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of Federal law, the accuracy of information obtained or introduced occasionally may be unclear or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of an investigation, thereby interfering with the related investigation and law enforcement activities.

(e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information would impede law enforcement in that it could compromise investigations by: Revealing the existence of an otherwise confidential investigation and thereby provide an opportunity for the subject of an investigation to conceal evidence, alter patterns of behavior, or take other actions that could thwart investigative efforts; reveal the identity of witnesses in investigations, thereby providing an opportunity for the subjects of the investigations or others to harass, intimidate, or otherwise interfere with the collection of evidence or other information from such witnesses; or reveal the identity of

confidential informants, which would negatively affect the informant's usefulness in any ongoing or future investigations and discourage members of the public from cooperating as confidential informants in any future investigations.

(f) From subsections (e)(4)(G) and (H) (Agency Requirements), and (f) (Agency Rules) because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

(g) From subsection (e)(5) (Collection of Information) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.

(h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS' ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal, and could result in disclosure of investigative techniques, procedures, and evidence.

(i) From subsection (g) to the extent that the system is exempt from other specific subsections of the Privacy Act relating to individuals' rights to access and amend their records contained in the system. Therefore DHS is not required to establish rules or procedures pursuant to which individuals may seek a civil remedy for the agency's: Refusal to amend a record; refusal to comply with a request for access to records; failure to maintain accurate, relevant, timely and complete records; or failure to otherwise comply with an individual's right to access or amend records.

31. The DHS/ICE—010 Confidential and Other Sources of Information (COSI) system of records consists of electronic and paper records and will be used by DHS and its components. The DHS/ICE—010 Confidential and Other Sources of Information system is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to: the enforcement of civil and criminal laws; and investigations, inquiries, and proceedings there under; and national security

and intelligence activities. The DHS/ICE—010 Confidential and Other Sources of Information system contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other Federal, State, local, tribal, foreign, or international government agencies. The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(5) and (e)(8); (f), and (g) pursuant to 5 U.S.C. 552a(j)(2). Additionally, the Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), and (f) pursuant to 5 U.S.C. 552a(k)(2). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation, and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, to the existence of the investigation, and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an impossible administrative burden by requiring investigations to be continuously re-investigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential viola-

tions of Federal law, the accuracy of information obtained or introduced occasionally may be unclear or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of an investigation, thereby interfering with the related investigation and law enforcement activities.

(e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information would impede law enforcement in that it could compromise investigations by: Revealing the existence of an otherwise confidential investigation and thereby provide an opportunity for the subject of an investigation to conceal evidence, alter patterns of behavior, or take other actions that could thwart investigative efforts; reveal the identity of witnesses in investigations, thereby providing an opportunity for the subjects of the investigations or others to harass, intimidate, or otherwise interfere with the collection of evidence or other information from such witnesses; or reveal the identity of confidential informants, which would negatively affect the informant's usefulness in any ongoing or future investigations and discourage members of the public from cooperating as confidential informants in any future investigations.

(f) From subsections (e)(4)(G) and (H) (Agency Requirements), and (f) (Agency Rules) because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

(g) From subsection (e)(5) (Collection of Information) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.

(h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere

with DHS' ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal, and could result in disclosure of investigative techniques, procedures, and evidence.

(i) From subsection (g) to the extent that the system is exempt from other specific subsections of the Privacy Act relating to individuals' rights to access and amend their records contained in the system. Therefore DHS is not required to establish rules or procedures pursuant to which individuals may seek a civil remedy for the agency's: Refusal to amend a record; refusal to comply with a request for access to records; failure to maintain accurate, relevant, timely and complete records; or failure to otherwise comply with an individual's right to access or amend records.

32. The DHS/USCIS—006 Fraud Detection and National Security Data System (FDNS—DS) system of records consists of a stand alone database and paper files that will be used by DHS and its components. The DHS/USCIS—006 Fraud Detection and National Security Data System is a case management system used to record, track, and manage immigration inquiries, investigative referrals, law enforcement requests, and case determinations involving benefit fraud, criminal activity, public safety and national security concerns. The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f) pursuant to 5 U.S.C. 552a(k)(2). These exemptions apply only to the extent that records in the system are subject to exemption pursuant to 5 U.S.C. 552a(k)(2). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation; and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory viola-

tion, to the existence of the investigation, and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an impossible administrative burden by requiring investigations to be continuously re-investigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of Federal law, the accuracy of information obtained or introduced occasionally may be unclear or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsections (e)(4)(G) and (e)(4)(H) (Agency Requirements) because portions of this system are exempt from the individual access provisions of subsection (d) which exempts providing access because it could alert a subject to the nature or existence of an investigation, and thus there could be no procedures for that particular data. Procedures do exist for access for those portions of the system that are not exempted.

(e) From subsection (e)(4)(I) (Agency Requirements) because providing such source information would impede law enforcement or intelligence by compromising the nature or existence of a confidential investigation.

(f) From subsection (f) (Agency Rules) because portions of this system are exempt from the access and amendment provisions of subsection (d).

33. The DHS/USCG—028 Family Advocacy Case Records system of records consists of electronic and paper records and will be used by DHS and its components. The DHS/USCG—028 Family Advocacy Case Records is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to: the enforcement of civil and criminal laws; investigations, inquiries, and proceedings there under. The DHS/USCG—028 Family Advocacy Case Records contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other Federal, State, local, tribal, foreign, or international government agencies. The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations

set forth in 5 U.S.C. 552a (c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f) pursuant to 5 U.S.C. 552a(k)(2). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation, and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, to the existence of the investigation, and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an impossible administrative burden by requiring investigations to be continuously re-investigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of Federal law, the accuracy of information obtained or introduced occasionally may be unclear or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsections (e)(4)(G), (H), and (I) (Agency Requirements), and (f) (Agency Rules) because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures

pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

34. The DHS/USCG–029 Notice of Arrival and Departure System of Records consists of electronic and paper records and will be used by DHS and its components. The DHS/USCG–029 Notice of Arrival and Departure System of Records is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to the enforcement of civil and criminal laws; investigations, inquiries, and proceedings there under. The DHS/USCG–029 Notice of Arrival and Departure System of Records contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other federal, state, local, tribal, foreign, or international government agencies.

The Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(j)(2), exempted this system from the following provisions of the Privacy Act: Sections (c)(3), (e)(8), and (g) of the Privacy Act of 1974, as amended, as is necessary and appropriate to protect this information. Further, DHS has exempted section (c)(3) of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(k)(2), as is necessary and appropriate to protect this information.

Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process. When an investigation has been completed, information on disclosures made may continue to be exempted if the fact that an investigation occurred remains sensitive after completion.

(b) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS's ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under

seal and could result in disclosure of investigative techniques, procedures, and evidence.

(c) From subsection (g)(1) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act.

35. The DHS/Secret Service—001 Criminal Investigation Information system of records consists of electronic and paper records and will be used by DHS and its components. The DHS/Secret Service—001 Criminal Investigation Information system is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to: The enforcement of civil and criminal laws; investigations, inquiries, and proceedings there under; the protection of the President of the United States or other individuals and locations pursuant to section 3056 and 3056A of Title 18. The DHS/Secret Service—001 Criminal Investigation Information system contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other Federal, State, local, tribal, foreign, international government agencies, as well as private corporate, education and other entities. The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5) and (e)(8); (f), and (g) pursuant to 5 U.S.C. 552a(j)(2). Additionally, the Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (I), and (f) pursuant to 5 U.S.C. 552a(k)(1), (k)(2), and (k)(3). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation, or protective inquiry, and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or the Secret Service's protective mission. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, or inquiry, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative or inquiry process.

(b) From subsection (d) (Access to Records) because access to the records contained in

this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, or protective inquiry to the existence of the investigation or inquiry, and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation or inquiry, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement or protective activities and/or could disclose security-sensitive information that could be detrimental to homeland security or the protective mission of the Secret Service.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of Federal law or protective inquiries, the accuracy of information obtained or introduced occasionally may be unclear or the information may not be strictly relevant or necessary to a specific investigation or protective inquiry. In the interests of effective law enforcement, and/or the protective mission of the Secret Service, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity, or a threat to an individual, location or event protected or secured by the Secret Service.

(d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation or protective inquiry would alert the subject to the nature or existence of an investigation or inquiry, thereby interfering with the related investigation or inquiry and law enforcement or protective activities.

(e) From subsection (e)(3) (Notice to Individuals Providing Information) because providing such detailed information would impede law enforcement or protective activities in that it could compromise investigations or inquires by: Revealing the existence of an otherwise confidential investigation or inquiry and thereby provide an opportunity for the subject of an investigation or inquiry to conceal evidence, alter patterns of behavior, or take other actions that could thwart investigative or protective efforts; reveal the identity of witnesses in investigations or inquiries, thereby providing an opportunity for the subjects of the investigations or inquiries or others to harass, intimidate, or otherwise interfere with the collection of evidence or other information from such witnesses; or reveal the identity of confidential informants, which would negatively affect the informant's usefulness in any ongoing or future investigations or protective activities and discourage members of the public from cooperating as confidential informants in

any future investigations or protective activities.

(f) From subsections (e)(4)(G), (H), and (I) (Agency Requirements), and (f) (Agency Rules) because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to the existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative or protective efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

(g) From subsection (e)(5) (Maintenance of Information Used in Making any Determination) because in the collection of information for law enforcement and protective purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with (e)(5) would preclude Secret Service DHS agents from using their investigative and protective training and exercising good judgment to both conduct and report on investigations or other protective activities.

(h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS' ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal, or/and could result in disclosure of investigative or protective techniques, procedures, and evidence.

(i) From subsection (g) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act relating to individuals' rights to access and amend their records contained in the system. Therefore DHS is not required to establish rules or procedures pursuant to which individuals may seek a civil remedy for the agency's: Refusal to amend a record; refusal to comply with a request for access to records; failure to maintain accurate, relevant, timely and complete records; or failure to otherwise comply with an individual's right to access or amend records.

36. The DHS/Secret Service—003 Non-Criminal Investigation Information system of records consists of electronic and paper records and will be used by DHS and its components. The DHS/Secret Service—003 Non-Criminal Investigation Information system is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to: The enforcement of civil and criminal laws; criminal, civil, protective and background investigations and inquiries, and proceedings thereunder; the protection of the President of the United States or other indi-

viduals and locations pursuant to section 3056 and 3056A of Title 18; and the hiring of employees through an application process which includes the use of polygraph examinations. The DHS/Secret Service—003 Non-Criminal Investigation Information system contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other Federal, State, local, tribal, foreign, or international government agencies, as well as private corporate, educational and other entities. The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5) and (e)(8); (f), and (g) pursuant to 5 U.S.C. 552a(j)(2). Additionally, the Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f) pursuant to 5 U.S.C. 552a(k)(1), (k)(2), (k)(3), (k)(5), and (k)(6). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation, or protective inquiry, and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or the Secret Service's protective mission. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation or inquiry, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative or inquiry process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, or protective inquiry to the existence of the investigation or inquiry, and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation or inquiry, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement or protective activities and/or could disclose security-sensitive information that

could be detrimental to homeland security or the protective mission of the Secret Service.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of Federal law or protective inquiries, the accuracy of information obtained or introduced occasionally may be unclear or the information may not be strictly relevant or necessary to a specific investigation or protective inquiry. In the interests of effective law enforcement and/or the protective mission of the Secret Service, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity, or a threat to an individual, location or event protected or secured by the Secret Service.

(d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation or protective inquiry would alert the subject to the nature or existence of an investigation or inquiry, thereby interfering with the related investigation or inquiry and law enforcement or protective activities.

(e) From subsection (e)(3) (Notice to Individuals Providing Information) because providing such detailed information would impede law enforcement or protective activities in that it could compromise investigations or inquiries by: Revealing the existence of an otherwise confidential investigation or inquiry and thereby provide an opportunity for the subject of an investigation or inquiry to conceal evidence, alter patterns of behavior, or take other actions that could thwart investigative or protective efforts; reveal the identity of witnesses in investigations or inquiries, thereby providing an opportunity for the subjects of the investigations or inquiries or others to harass, intimidate, or otherwise interfere with the collection of evidence or other information from such witnesses; or reveal the identity of confidential informants, which would negatively affect the informant's usefulness in any ongoing or future investigations or protective activities and discourage members of the public from cooperating as confidential informants in any future investigations or protective activities.

(f) From subsections (e)(4)(G), (H), and (I) (Agency Requirements), and (f) (Agency Rules) because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to the existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative or

protective efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

(g) From subsection (e)(5) (Maintenance of Information Used in Making any Determination) because in the collection of information for law enforcement and protective purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with (e)(5) would preclude Secret Service agents from using their investigative and protective training, and exercising good judgment to both conduct and report on investigations or other protective activities.

(h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS' ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal, or could result in disclosure of investigative or protective techniques, procedures, and evidence.

(i) From subsection (g) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act relating to individuals' rights to access and amend their records contained in the system. Therefore DHS is not required to establish rules or procedures pursuant to which individuals may seek a civil remedy for the agency's: Refusal to amend a record; refusal to comply with a request for access to records; failure to maintain accurate, relevant, timely and complete records; or failure to otherwise comply with an individual's right to access or amend records.

37. The DHS/Secret Service—004 Protection Information system of records consists of electronic and paper records and will be used by DHS and its components. The DHS/Secret Service—004 Protection Information system is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to: the enforcement of civil and criminal laws; investigations, inquiries, and proceedings thereunder; and the protection of the President of the United States or other individuals and locations pursuant to Sections 3056 and 3056A of Title 18. The DHS/Secret Service—004 Protection Information system contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other Federal, State, local, Tribal, foreign, or international government agencies, as well as private corporate or other entities. The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5) and (e)(8); (f), and (g) pursuant to 5 U.S.C. 552a(j)(2). Additionally, the Secretary of

Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a (c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f) pursuant to 5 U.S.C. 552a(k)(1), (k)(2), and (k)(3). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation or a protective inquiry to the existence of the investigation or inquiry, and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or the Secret Service's protective mission. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation or inquiry, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative or inquiry process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, or protective inquiry to the existence of the investigation or inquiry, and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, or inquiry to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations, law enforcement or protective activities and/or could disclose security-sensitive information that could be detrimental to homeland security or the protective mission of the Secret Service.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of Federal law or protective inquiries, the accuracy of information obtained or introduced occasionally may be unclear or the information may not be strictly relevant or necessary to a specific investigation or protective inquiry. In the interests of effective law enforcement and/or the protective mission of the Secret Service, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity, or a possible threat to an individual, location or event protected or secured by the Secret Service.

(d) From subsection (e)(2) (Collection of Information from Individuals) because requir-

ing that information be collected from the subject of an investigation or protective inquiry would alert the subject to the nature or existence of an investigation or inquiry, thereby interfering with the related investigation or inquiry and law enforcement or protective activities.

(e) From subsection (e)(3) (Notice to Individuals Providing Information) because providing such detailed information would impede law enforcement or protective activities in that it could compromise investigations or inquiries by: Revealing the existence of an otherwise confidential investigation or inquiry and thereby provide an opportunity for the subject of an investigation or inquiry to conceal evidence, alter patterns of behavior, or take other actions that could thwart investigative or protective efforts; reveal the identity of witnesses, thereby providing an opportunity for the subjects of the investigations or inquiries or others to harass, intimidate, or otherwise interfere with the collection of evidence or other information from such witnesses; or reveal the identity of confidential informants, which would negatively affect the informant's usefulness in any ongoing or future investigations or protective activities and discourage members of the public from cooperating as confidential informants in any future investigations or protective activities.

(f) From subsections (e)(4)(G), (H), and (I) (Agency Requirements), and (f) (Agency Rules) because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to the existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative and protective efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

(g) From subsection (e)(5) (Maintenance of Information Used in Making any Determination) because in the collection of information for law enforcement and protective purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with (e)(5) would preclude Secret Service agents from using their investigative and protective training and exercising good judgment to both conduct and report on investigations or other protective activities.

(h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS' ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under

seal, and could result in disclosure of investigative or protective techniques, procedures, and evidence.

(i) From subsection (g) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act relating to individuals' rights to access and amend their records contained in the system. Therefore DHS is not required to establish rules or procedures pursuant to which individuals may seek a civil remedy for the agency's: refusal to amend a record; refusal to comply with a request for access to records; failure to maintain accurate, relevant, timely and complete records; or failure to otherwise comply with an individual's right to access or amend records.

38. The DHS/ALL—025 Law Enforcement Authority in Support of the Protection of Property Owned or Occupied by the Department of Homeland Security system of records consists of electronic and paper records and will be used by DHS and its components. The DHS/ALL—025 Law Enforcement Authority in Support of the Protection of Property Owned or Occupied by the Department of Homeland Security system is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to: The enforcement of civil and criminal laws; investigations, inquiries, and proceedings there under; and national security and intelligence activities. The DHS/ALL—025 Law Enforcement Authority in Support of the Protection of Property Owned or Occupied by the Department of Homeland Security system contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other Federal, State, local, tribal, foreign, or international government agencies. The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a (c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f) pursuant to 5 U.S.C. 552a(k)(1), (k)(2), and (k)(5). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation, and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a

record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, to the existence of the investigation, and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an impossible administrative burden by requiring investigations to be continuously re-investigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of Federal law, the accuracy of information obtained or introduced occasionally may be unclear or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsections (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements), and (f) (Agency Rules) because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

39. The DHS/ALL—017 General Legal Records system of records consists of electronic and paper records and will be used by DHS and its components. The DHS/ALL—017 General Legal Records system of records is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to: The enforcement of civil and criminal laws; investigations, inquiries, and proceedings thereunder; national security and intelligence activities; and protection of the President of the United States or other individuals pursuant to section 3056 and 3056A of

Title 18. The DHS/ALL—017 General Legal Records system of records contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other Federal, State, local, tribal, foreign, or international government agencies. The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5) and (e)(8); (f), and (g), pursuant to exemption 5 U.S.C. 552a(j)(2). Additionally, the Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a (c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (I), and (f), pursuant to 5 U.S.C. 552a(k)(1), (k)(2), (k)(3) and (k)(5). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation, and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, to the existence of the investigation, and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an impossible administrative burden by requiring investigations to be continuously re-investigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential viola-

tions of Federal law, the accuracy of information obtained or introduced occasionally may be unclear or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of an investigation, thereby interfering with the related investigation and law enforcement activities.

(e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information would impede law enforcement in that it could compromise investigations by: Revealing the existence of an otherwise confidential investigation and thereby provide an opportunity for the subject of an investigation to conceal evidence, alter patterns of behavior, or take other actions that could thwart investigative efforts; reveal the identity of witnesses in investigations, thereby providing an opportunity for the subjects of the investigations or others to harass, intimidate, or otherwise interfere with the collection of evidence or other information from such witnesses; or reveal the identity of confidential informants, which would negatively affect the informant's usefulness in any ongoing or future investigations and discourage members of the public from cooperating as confidential informants in any future investigations.

(f) From subsections (e)(4)(G), (H), and (I) (Agency Requirements), and (f) (Agency Rules) because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

(g) From subsection (e)(5) (Collection of Information) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.

(h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere

with DHS' ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal, and could result in disclosure of investigative techniques, procedures, and evidence.

(i) From subsection (g) to the extent that the system is exempt from other specific subsections of the Privacy Act relating to individuals' rights to access and amend their records contained in the system. Therefore DHS is not required to establish rules or procedures pursuant to which individuals may seek a civil remedy for the agency's: Refusal to amend a record; refusal to comply with a request for access to records; failure to maintain accurate, relevant, timely and complete records; or failure to otherwise comply with an individual's right to access or amend records.

40. The DHS/ALL—023 Personnel Security Management system of records consists of electronic and paper records and will be used by DHS and its components. The DHS/ALL—023 Personnel Security Management system is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to: The enforcement of civil and criminal laws; investigations, inquiries, and proceedings thereunder; national security and intelligence activities; and protection of the President of the United States or other individuals pursuant to section 3056 and 3056A of Title 18. The DHS/ALL—023 Personnel Security Management system contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other Federal, State, local, tribal, foreign, or international government agencies. The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a (c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f) pursuant to 5 U.S.C. 552a(k)(1), (k)(2), (k)(3), and (k)(5). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation, and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid

detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, to the existence of the investigation, and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an impossible administrative burden by requiring investigations to be continuously re-investigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of Federal law, the accuracy of information obtained or introduced occasionally may be unclear or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsections (e)(4)(G), (H), and (I) (Agency Requirements), and (f) (Agency Rules) because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

41. The DHS/NPPD/US—VISIT—001 Arrival and Departure Information system of records notice is a system for the storage and use of biographic, biometric indicator, and encounter data consolidated from various systems regarding aliens who have applied for entry, entered, or departed the United States. Information in the DHS/NPPD/US—VISIT—001 Arrival and Departure Information system of records notice is used primarily to facilitate the investigation of subjects of interest who may have violated their immigration status by remaining in the United States beyond their authorized stay; thereby supporting the several and varied missions and functions of DHS, including but not limited to:

the enforcement of civil and criminal laws (including the immigration law); investigations, inquiries; national security and intelligence activities in support of the DHS mission to identify and prevent acts of terrorism against the United States. The information is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other Federal, State, local, tribal, foreign, or international government agencies. The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(5) and (e)(8); (f); and (g) pursuant to 5 U.S.C. 552a(j)(2). Additionally, the Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H); and (f) pursuant to 5 U.S.C. 552a(k)(1), (k)(2), (k)(3) and (k)(5). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation; and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, to the existence of the investigation, and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an impossible administrative burden by requiring investigations to be continuously re-investigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of Federal law, the accuracy of information obtained or introduced occasionally may be unclear or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of an investigation, thereby interfering with the related investigation and law enforcement activities.

(e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information would impede law enforcement in that it could compromise investigations by: revealing the existence of an otherwise confidential investigation and thereby provide an opportunity for the subject of an investigation to conceal evidence, alter patterns of behavior, or take other actions that could thwart investigative efforts; reveal the identities of witnesses in investigations, thereby providing an opportunity for the subjects of the investigations or others to harass, intimidate, or otherwise interfere with the collection of evidence or other information from such witnesses; or reveal the identity of confidential informants, which would negatively affect the informant's usefulness in any ongoing or future investigations and discourage members of the public from cooperating as confidential informants in any future investigations.

(f) From subsections (e)(4)(G) and (H) (Agency Requirements), and (f) (Agency Requirements) because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

(g) From subsection (e)(5) (Collection of Information) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment

to both conduct and report on investigations.

(h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS' ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal, and could result in disclosure of investigative techniques, procedures, and evidence.

(i) From subsection (g) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act relating to individuals' rights to access and amend their records contained in the system. Therefore DHS is not required to establish rules or procedures pursuant to which individuals may seek a civil remedy for the agency's: refusal to amend a record; refusal to comply with a request for access to records; failure to maintain accurate, relevant, timely and complete records; or failure to otherwise comply with an individual's right to access or amend records.

42. The DHS/NPPD/US-VISIT-003 Technical Reconciliation Analysis Classification system of records (TRACS) consists of stand alone database and paper files that will be used by DHS and its components. This system of records will be used to perform a range of information management and analytic functions involving collecting, verifying, and resolving tracking of data primarily on individuals who are not United States citizens or legal permanent residents (LPRs). However, it will contain data on: (1.) U.S. citizens or LPRs who have a connection to the DHS mission (e.g., individuals who have submitted a visa application to the UK, or have made requests for a license or credential as part of a background check or security screening in connection with their hiring or retention, performance of a job function or the issuance of a license or credential for employment at DHS); (2.) U.S. citizens and LPRs who have an incidental connection to the DHS mission (e.g., individuals living at the same address as individuals who have remained in this country beyond their authorized stays); and (3.) individuals who have, over time, changed their status and became U.S. citizens or LPRs. The DHS/NPPD/US-VISIT-003 Technical Reconciliation Analysis Classification system of records is managed and maintained by the US-VISIT Program. The data contained in the DHS/NPPD/US-VISIT-003 Technical Reconciliation Analysis Classification system of records is primarily derived from DHS/NPPD/U.S-VISIT-001 Arrival and Departure Information System (ADIS); DHS/CBP-011 TECS; DHS/ICE-001 Student and Exchange Visitor Information System (SEVIS); DHS/ICE/CBP/USCIS-001-03 Enforcement Operational Immigration Records (ENFORCE/IDENT); DHS/ICE-011 Removable Alien Records System (RARS); DHS/

USCIS-001 Alien File (A-File) and Central Index System (CIS); DHS/USCIS-007 Benefits Information System covering Computer Linked Application Information Management System 3 (Claims 3) and Computer Linked Application Information Management System 4 (Claims 4); DHS/USCIS Refugees, Asylum & Parole System (RAPS); and from the Department of State's Consolidated Consular Database (CCD). The DHS/NPPD/US-VISIT-003 Technical Reconciliation Analysis Classification system of records also contains data from web searches for addresses and phone numbers. This data is collected by, on behalf of, in support of, or in cooperation with DHS and its components. The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5) and (e)(8); (f); and (g) pursuant to 5 U.S.C. 552a(j)(2). Additionally, the Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f) pursuant to 5 U.S.C. 552a(k)(1), (k)(2), and (k)(5). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation, and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, to the existence of the investigation, and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an

impossible administrative burden by requiring investigations to be continuously re-investigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of Federal law, the accuracy of information obtained or introduced occasionally may be unclear or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of an investigation, thereby interfering with the related investigation and law enforcement activities.

(e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information would impede law enforcement in that it could compromise investigations by: revealing the existence of an otherwise confidential investigation and thereby provide an opportunity for the subject of an investigation to conceal evidence, alter patterns of behavior, or take other actions that could thwart investigative efforts; reveal the identity of witnesses in investigations, thereby providing an opportunity for the subjects of the investigations or others to harass, intimidate, or otherwise interfere with the collection of evidence or other information from such witnesses; or reveal the identity of confidential informants, which would negatively affect the informant's usefulness in any ongoing or future investigations and discourage members of the public from cooperating as confidential informants in any future investigations.

(f) From subsections (e)(4)(G), and (e)(4)(H) (Agency Requirements) because portions of this system are exempt from the individual access provisions of subsection (d) which exempts providing access because it could alert a subject to the nature or existence of an investigation, and thus there could be no procedures for that particular data. Procedures do exist for access for those portions of the system that are not exempted.

(g) From subsection (e)(4)(I) (Agency Requirements) because providing such source information would impede enforcement or intelligence by compromising the nature or existence of a confidential investigation.

(h) From subsection (e)(5) (Collection of Information) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and

complete. Compliance with (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.

(i) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS' ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal, and could result in disclosure of investigative techniques, procedures and evidence.

(j) From subsection (f) (Agency Rules) because portions of this system are exempt from the access and amendment provisions of subsection (d).

(k) From subsection (g) to the extent that the system is exempt from other specific subsections of the Privacy Act.

43. The DHS/USCG—013 Marine Information for Safety and Law Enforcement system of records consists of electronic and paper records and will be used by DHS and its components. The DHS/USCG—013 Marine Information for Safety and Law Enforcement system of records is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to: the enforcement of civil and criminal laws; investigations, inquiries, and proceedings there under; national security and intelligence activities. The DHS/USCG—013 Marine Information for Safety and Law Enforcement system of records contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other Federal, State, local, tribal, foreign, or international government agencies. The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5) and (e)(8); (f); and (g) pursuant to 5 U.S.C. 552a(j)(2). Additionally, the Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H); (I); and (f) pursuant to 5 U.S.C. 552a(k)(2). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation, and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore

present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, to the existence of the investigation, and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an impossible administrative burden by requiring investigations to be continuously re-investigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of Federal law, the accuracy of information obtained or introduced occasionally may be unclear or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of an investigation, thereby interfering with the related investigation and law enforcement activities.

(e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information would impede law enforcement in that it could compromise investigations by: revealing the existence of an otherwise confidential investigation and thereby provide an opportunity for the subject of an investigation to conceal evidence, alter patterns of behavior, or take other actions that could thwart investigative efforts; reveal the identity of witnesses in investigations, thereby providing an opportunity for the subjects of the investigations or others to harass, intimidate, or otherwise interfere with the collection of evidence or other information from such witnesses; or reveal the identity of confidential informants, which would negatively affect the informant's usefulness in

any ongoing or future investigations and discourage members of the public from cooperating as confidential informants in any future investigations.

(f) From subsections (e)(4)(G), (H), and (I) (Agency Requirements), and (f) (Agency Rules) because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

(g) From subsection (e)(5) (Collection of Information) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.

(h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS' ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal, and could result in disclosure of investigative techniques, procedures, and evidence.

(i) From subsection (g) to the extent that the system is exempt from other specific subsections of the Privacy Act relating to individuals' rights to access and amend their records contained in the system. Therefore DHS is not required to establish rules or procedures pursuant to which individuals may seek a civil remedy for the agency's: refusal to amend a record; refusal to comply with a request for access to records; failure to maintain accurate, relevant timely and complete records; or failure to otherwise comply with an individual's right to access or amend records.

44. The DHS/USCG—030 Merchant Seaman's Records system of records consists of electronic and paper records and will be used by DHS and its components. The DHS/USCG—030 Merchant Seaman's Records system of records is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to: the enforcement of civil and criminal laws; investigations, inquiries, and proceedings there under. The DHS/USCG—030 Merchant Seaman's Records system of records contains information that is collected by, on behalf of, in support of, or in

cooperation with DHS and its components and may contain personally identifiable information collected by other Federal, State, local, tribal, foreign, or international government agencies. The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f) pursuant to 5 U.S.C. 552a(k)(2). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation, and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, to the existence of the investigation, and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an impossible administrative burden by requiring investigations to be continuously re-investigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of Federal law, the accuracy of information obtained or introduced occasionally may be unclear or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsections (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements), and (f) (Agency Rules) because portions of this system are exempt from the individual access

provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

45. The DHS/CBP—006 Automated Targeting system of records performs screening of both inbound and outbound cargo, travelers, and conveyances. As part of this screening function and to facilitate DHS's border enforcement mission, the DHS/CBP—006 Automated Targeting system of records compares information received with CBP's law enforcement databases, the Federal Bureau of Investigation Terrorist Screening Center's Terrorist Screening Database (TSDB), information on outstanding warrants or warrants, information from other government agencies regarding high-risk parties, and risk-based rules developed by analysts using law enforcement data, intelligence, and past case experience. The modules also facilitate analysis of the screening results of these comparisons. This supports the several and varied missions and functions of DHS, including but not limited to: The enforcement of civil and criminal laws (including the immigration law); investigations, inquiries; national security and intelligence activities in support of the DHS mission to identify and prevent acts of terrorism against the United States. The information is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other Federal, State, local, tribal, foreign, or international government agencies. Certain records or information in DHS/CBP—006 Automated Targeting system of records are exempt from the Privacy Act. With respect to the ATS-P module, exempt records are the targeting rule sets, risk assessment analyses, and business confidential information contained in the PNR that relates to the air and vessel carriers. No exemption shall be asserted regarding PNR data about the requester, provided by either the requester or a booking agent, brokers, or another person on the requester's behalf. This information, upon request, may be provided to the requester in the form in which it was collected from the respective carrier, but may not include certain business confidential information of the air carrier that is also contained in the record, such as use and application of frequent flier miles, internal annotations to the air fare, etc. For other DHS/CBP—006 Automated Targeting system of records modules

the only information maintained in the system is the targeting rule sets, risk assessment analyses, and a pointer to the data from the source system of records. The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (4)(G) through (I), (e)(5), and (8); (f); and (g) pursuant to 5 U.S.C. 552a(j)(2). Additionally, the Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (4)(G) through (I), (e)(5), and (8); (f); and (g) pursuant to 5 U.S.C. 552a(k)(2). These exemptions also apply to the extent that information in this system of records is recompiled or is created from information contained in other systems of records. After conferring with the appropriate component or agency, DHS may waive applicable exemptions in appropriate circumstances and where it would not appear to interfere with or adversely affect the law enforcement purposes of the systems from which the information is recompiled or in which it is contained. Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (4) (Accounting for Disclosure) because making available to a record subject the accounting of disclosures from records concerning him or her would specifically reveal any investigative interest in the individual. Revealing this information could reasonably be expected to compromise ongoing efforts to investigate a known or suspected criminal or terrorist, or other person of interest, by notifying the record subject that he or she is under investigation. This information could also permit the record subject to take measures to impede the investigation, e.g., destroy evidence, intimidate potential witnesses, or flee the area to avoid or impede the investigation. Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons: (a) From subsection (c)(3) (Accounting for Disclosure) because making available to a record subject the accounting of disclosures from records concerning him or her would specifically reveal any investigative interest in the individual. Revealing this information could reasonably be expected to compromise ongoing efforts to investigate a known or suspected terrorist by notifying the record subject that he or she is under investigation. This information could also permit the record subject to take measures to impede the investigation, e.g., destroy evidence, intimidate po-

tential witnesses, or flee the area to avoid or impede the investigation.

(b) From subsection (c)(4) (Accounting for Disclosure, notice of dispute) because certain records in this system are exempt from the access and amendment provisions of subsection (d), this requirement to inform any person or other agency about any correction or notation of dispute that the agency made with regard to those records, should not apply.

(c) From subsections (d)(1), (2), (3), and (4) (Access to Records) because these provisions concern individual access to and amendment of certain records contained in this system, including law enforcement, counterterrorism, and investigatory records. Compliance with these provisions could alert the subject of an investigation to the fact and nature of the investigation, and/or the investigative interest of intelligence or law enforcement agencies; compromise sensitive information related to law enforcement, including matters bearing on national security; interfere with the overall law enforcement process by leading to the destruction of evidence, improper influencing of witnesses, fabrication of testimony, and/or flight of the subject; could identify a confidential source; reveal a sensitive investigative or intelligence technique; or constitute a potential danger to the health or safety of law enforcement personnel, confidential informants, and witnesses. Amendment of these records would interfere with ongoing counterterrorism or law enforcement investigations and analysis activities and impose an impossible administrative burden by requiring investigations, analyses, and reports to be continuously reinvestigated and revised.

(d) From subsection (e)(1) (Relevancy and Necessity of Information) because it is not always possible for DHS or other agencies to know in advance what information is relevant and necessary for it to complete screening of cargo, conveyances, and passengers. Information relating to known or suspected criminals or terrorists or other persons of interest, is not always collected in a manner that permits immediate verification or determination of relevancy to a DHS purpose. For example, during the early stages of an investigation, it may not be possible to determine the immediate relevancy of information that is collected—only upon later evaluation or association with further information, obtained subsequently, may it be possible to establish particular relevance to a law enforcement program. Lastly, this exemption is required because DHS and other agencies may not always know what information about an encounter with a known or suspected criminal or terrorist or other person of interest will be relevant to law enforcement for the purpose of conducting an operational response.

(e) From subsection (e)(2) (Collection of Information from Individuals) because application of this provision could present a serious impediment to counterterrorism or other law enforcement efforts in that it would put the subject of an investigation, study or analysis on notice of that fact, thereby permitting the subject to engage in conduct designed to frustrate or impede that activity. The nature of counterterrorism, and law enforcement investigations is such that vital information about an individual frequently can be obtained only from other persons who are familiar with such individual and his/her activities. In such investigations it is not feasible to rely solely upon information furnished by the individual concerning his own activities.

(f) From subsection (e)(3) (Notice to Subjects), to the extent that this subsection is interpreted to require DHS to provide notice to an individual if DHS or another agency receives or collects information about that individual during an investigation or from a third party. Should the subsection be so interpreted, exemption from this provision is necessary to avoid impeding counterterrorism or other law enforcement efforts by putting the subject of an investigation, study or analysis on notice of that fact, thereby permitting the subject to engage in conduct intended to frustrate or impede that activity.

(g) From subsections (e)(4)(G), (H) and (I) (Agency Requirements) because portions of this system are exempt from the access and amendment provisions of subsection (d).

(h) From subsection (e)(5) (Collection of Information) because many of the records in this system coming from other systems of records are derived from other domestic and foreign agency record systems and therefore it is not possible for DHS to vouch for their compliance with this provision; however, the DHS has implemented internal quality assurance procedures to ensure that data used in its screening processes is as complete, accurate, and current as possible. In addition, in the collection of information for law enforcement and counterterrorism purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light. The restrictions imposed by (e)(5) would limit the ability of those agencies' trained investigators and intelligence analysts to exercise their judgment in conducting investigations and impede the development of intelligence necessary for effective law enforcement and counterterrorism efforts.

(i) From subsection (e)(8) (Notice on Individuals) because to require individual notice of disclosure of information due to compulsory legal process would pose an impossible

administrative burden on DHS and other agencies and could alert the subjects of counterterrorism or law enforcement investigations to the fact of those investigations when not previously known.

(j) From subsection (f) (Agency Rules) because portions of this system are exempt from the access and amendment provisions of subsection (d). Access to, and amendment of, system records that are not exempt or for which exemption is waived may be obtained under procedures described in the related SORN or subpart B of this part.

(k) From subsection (g) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act.

46. The DHS/CBP-007 Border Crossing Information System of Records consists of electronic and paper records and will be used by DHS and its Components. The DHS/CBP-007 Border Crossing Information System of Records is a repository of information held by DHS in connection with its several and varied missions and functions including, but not limited to the enforcement of civil and criminal laws; investigations, inquiries, and proceedings thereunder; and law enforcement, border security, and intelligence activities. The DHS/CBP-007 Border Crossing Information System of Records contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its Components and may contain personally identifiable information collected by other Federal, State, local, tribal, foreign, or international government agencies. At the time of border crossing and during the process of determining admissibility, CBP collects two types of data for which it claims different exemptions.

(a) CBP will not assert any exemption to limit an individual from accessing or amending his or her record with respect to information maintained in the system that is collected from a person at the time of crossing and submitted by that person's air, sea, bus, or rail carriers. The Privacy Act requires DHS to maintain an accounting of the disclosures made pursuant to all routine uses. Pursuant to 5 U.S.C. 552a(j)(2), CBP will not disclose the fact that a law enforcement or intelligence agency has sought particular records because it may affect ongoing law enforcement activities. The Secretary of Homeland Security has exempted this system from subsections (c)(3), (e)(8), and (g) of the Privacy Act of 1974, as amended, as is necessary and appropriate to protect this information. Further, DHS will claim exemption from subsection (c)(3) of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(k)(2) as is necessary and appropriate to protect this information. Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(i) From subsection (c)(3) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(ii) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS's ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal and could result in disclosure of investigative techniques, procedures, and evidence.

(iii) From subsection (g) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act.

(b) Additionally, this system contains records or information recompiled from or created from information contained in other systems of records that are exempt from certain provisions of the Privacy Act. For these records or information only, the Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(j)(2), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3), (c)(4); (d)(1)-(4); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5) and (e)(8); (f); and (g). Additionally, the Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(k)(2), has exempted this system from the following provisions of the Privacy Act, 5 U.S.C. 552a(c)(3); (d)(1)-(4); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(i) From subsection (c)(3) and (c)(4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(ii) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continually re-investigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(iii) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced occasionally may be unclear, or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(iv) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of the investigation, thereby interfering with that investigation and related law enforcement activities.

(v) From subsection (e)(3) (Notice to Subjects) because providing such detailed information could impede law enforcement by compromising the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(vi) From subsections (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements) and (f) (Agency Rules), because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, potential witnesses, and confidential informants.

(vii) From subsection (e)(5) (Collection of Information) because with the collection of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely,

and complete. Compliance with subsection (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.

(viii) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS's ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal and could result in disclosure of investigative techniques, procedures, and evidence.

(ix) From subsection (g) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act.

47. The Visa Security Program Records (VSPR) system of records consists of electronic and paper records and will be used by the Department of Homeland Security (DHS) U.S. Immigration and Customs Enforcement (ICE). VSPR consists of information created in support of the Visa Security Program, the purpose of which is to identify persons who may be ineligible for a U.S. visa because of criminal history, terrorism association, or other factors and convey that information to the State Department, which decides whether to issue the visa. VSPR contains records on visa applicants for whom a visa security review is conducted. VSPR contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other Federal, State, local, Tribal, foreign, or international government agencies. Pursuant to exemption 5 U.S.C. 552a(j)(2) of the Privacy Act, portions of this system are exempt from 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), and (e)(4)(H), (e)(5) and (e)(8); (f); and (g). Pursuant to 5 U.S.C. 552a(k)(1) and (k)(2), this system is exempt from the following provisions of the Privacy Act, subject to the limitations set forth in those subsections: 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), and (f). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the individual to the existence of an investigation in the form of a visa security review predicated on classified, national security, law enforcement, foreign government, or other sensitive information. Disclosure of the accounting would therefore present a serious impediment to ICE's Visa Security Program, immigration enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, thereby undermining the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could alert the individual to the existence of an investigation in the form of a visa security review predicated on classified, national security, law enforcement, foreign government, or other sensitive information. Revealing the existence of an otherwise confidential investigation could also provide the visa applicant an opportunity to conceal adverse information or take other actions that could thwart investigative efforts; and reveal the identity of other individuals with information pertinent to the visa security review, thereby providing an opportunity for the applicant to interfere with the collection of adverse or other relevant information from such individuals. Access to the records would therefore present a serious impediment to the enforcement of Federal immigration laws, law enforcement efforts and/or efforts to preserve national security. Amendment of the records could interfere with ICE's ongoing investigations and law enforcement activities and would impose an impossible administrative burden by requiring investigations to be continuously reinvestigated. In addition, permitting access and amendment to such information could disclose classified and other security-sensitive information that could be detrimental to national or homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations of visa applications, the accuracy of information obtained or introduced occasionally may be unclear or the information may not be strictly relevant or necessary to a specific investigation. In the interest of effective enforcement of Federal immigration laws, it is appropriate to retain all information that may be relevant to the determination whether an individual is eligible for a U.S. visa.

(d) From subsection (e)(2) (Collection of Information From Individuals) because requiring that information be collected from the visa applicant would alert the subject to the fact of an investigation in the form of a visa security review, and to the existence of adverse information about the individual, thereby interfering with the related investigation and law enforcement activities.

(e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information would impede immigration enforcement activities in that it could compromise investigations by: Revealing the existence of an otherwise confidential investigation and thereby provide an opportunity for the visa applicant to conceal adverse information, or take other actions that could thwart investigative efforts; Reveal the identity of other individuals with information pertinent to the visa security review, thereby providing an opportunity for the applicant to interfere

with the collection of adverse or other relevant information from such individuals; or reveal the identity of confidential informants, which would negatively affect the informant's usefulness in any ongoing or future investigations and discourage members of the public from cooperating as confidential informants in any future investigations.

(f) From subsections (e)(4)(G) and (H) (Agency Requirements), and (f) (Agency Rules) because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative and immigration enforcement efforts as described above.

(g) From subsection (e)(5) (Collection of Information) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.

(h) From subsection (e)(8) because to require individual notice of disclosure of information due to compulsory legal process would pose an impossible administrative burden on DHS and other agencies and could alert the subjects of counterterrorism, law enforcement, or intelligence investigations to the fact of those investigations when not previously known.

(i) From subsection (g) to the extent that the system is exempt from other specific subsections of the Privacy Act relating to individuals' rights to access and amend their records contained in the system. Therefore DHS is not required to establish rules or procedures pursuant to which individuals may seek a civil remedy for the agency's: Refusal to amend a record; refusal to comply with a request for access to records; failure to maintain accurate, relevant, timely and complete records; or failure to otherwise comply with an individual's right to access or amend records.

48. The DHS/ICE-011 Immigration and Enforcement Operational Records system of records consists of electronic and paper records and will be used by DHS and its components. The DHS/ICE-011 Immigration and Enforcement Operational Records system of records is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to: The enforcement of civil and

criminal laws; investigations, inquiries, and proceedings there under; and national security and intelligence activities. The DHS/ICE-011 Immigration and Enforcement Operational Records system of records contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other federal, state, local, tribal, foreign, or international government agencies. The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(5), and (e)(8); (f); and (g) pursuant to 5 U.S.C. 552a(j)(2). Additionally, the Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H); and (f) pursuant to 5 U.S.C. 552a(k)(2). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation, and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, to the existence of the investigation, and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an impossible administrative burden by requiring investigations to be continuously re-investigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of Federal law, the accuracy of information obtained or introduced occasionally may be unclear or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of an investigation, thereby interfering with the related investigation and law enforcement activities.

(e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information would impede law enforcement in that it could compromise investigations by: Revealing the existence of an otherwise confidential investigation and thereby provide an opportunity for the subject of an investigation to conceal evidence, alter patterns of behavior, or take other actions that could thwart investigative efforts; reveal the identity of witnesses in investigations, thereby providing an opportunity for the subjects of the investigations or others to harass, intimidate, or otherwise interfere with the collection of evidence or other information from such witnesses; or reveal the identity of confidential informants, which would negatively affect the informant's usefulness in any ongoing or future investigations and discourage members of the public from cooperating as confidential informants in any future investigations.

(f) From subsections (e)(4)(G) and (H) (Agency Requirements), and (f) (Agency Rules) because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

(g) From subsection (e)(5) (Collection of Information) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment

to both conduct and report on investigations.

(h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS' ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal, and could result in disclosure of investigative techniques, procedures, and evidence.

(i) From subsection (g) to the extent that the system is exempt from other specific subsections of the Privacy Act relating to individuals' rights to access and amend their records contained in the system. Therefore DHS is not required to establish rules or procedures pursuant to which individuals may seek a civil remedy for the agency's: Refusal to amend a record; refusal to comply with a request for access to records; failure to maintain accurate, relevant timely and complete records; or failure to otherwise comply with an individual's right to access or amend records.

49. The DHS/USCIS—009 Compliance Tracking and Management System of Records consists of electronic and paper files that will be used by DHS and its components. This system of records will be used to perform a range of information management and analytic functions involving minimizing misuse, abuse, discrimination, breach of privacy, and fraudulent use of SAVE and E-Verify. The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitation set forth in 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f) pursuant to 5 U.S.C. 552a(k)(2). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation, and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, to the existence of the investigation, and reveal investigative interest on the part

of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an impossible administrative burden by requiring investigations to be continuously re-investigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of Federal law, the accuracy of information obtained or introduced occasionally may be unclear or the information may not be strictly relevant or necessary to a specific investigation. In the interest of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsections (e)(4)(G), (H), and (I) (Agency Requirements), and (f) (Agency Rules) because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

50. The Immigration and Customs Enforcement (ICE)—006 Intelligence Records System (IIRS) consists of electronic and paper records and will be used by the Department of Homeland Security (DHS). IIRS is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to: the enforcement of civil and criminal laws; investigations, inquiries, and proceedings thereunder; and national security and intelligence activities. IIRS contains information that is collected by other federal and foreign government agencies and may contain personally identifiable information. Pursuant to exemption 5 U.S.C. 552a(j)(2) of the Privacy Act, portions of this system are exempt from 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(5) and (e)(8); (f), and (g). Pursuant to 5 U.S.C. 552a(k)(2), this system is exempt from the following provisions of the Privacy Act, subject to the limitations set forth in those subsections: 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), and (f). Exemptions from

these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation, and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, to the existence of the investigation, and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an impossible administrative burden by requiring investigations to be continuously re-investigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of Federal law, the accuracy of information obtained or introduced occasionally may be unclear or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of an investigation, thereby interfering with the related investigation and law enforcement activities.

(e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information would impede law enforcement in that it could compromise investigations by:

revealing the existence of an otherwise confidential investigation and thereby provide an opportunity for the subject of an investigation to conceal evidence, alter patterns of behavior, or take other actions that could thwart investigative efforts; reveal the identity of witnesses in investigations, thereby providing an opportunity for the subjects of the investigations or others to harass, intimidate, or otherwise interfere with the collection of evidence or other information from such witnesses; or reveal the identity of confidential informants, which would negatively affect the informant's usefulness in any ongoing or future investigations and discourage members of the public from cooperating as confidential informants in any future investigations.

(f) From subsections (e)(4)(G) and (H) (Agency Requirements), and (f) (Agency Rules) because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

(g) From subsection (e)(5) (Collection of Information) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.

(h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS' ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal, and could result in disclosure of investigative techniques, procedures, and evidence.

(i) From subsection (g) to the extent that the system is exempt from other specific subsections of the Privacy Act relating to individuals' rights to access and amend their records contained in the system. Therefore DHS is not required to establish rules or procedures pursuant to which individuals may seek a civil remedy for the agency's: refusal to amend a record; refusal to comply with a request for access to records; failure to maintain accurate, relevant timely and complete records; or failure to otherwise comply with an individual's right to access or amend records.

51. The DHS/ALL—027 The History of the Department of Homeland Security System of Records consists of electronic and paper records and will be used by DHS and its components. The DHS/ALL—027 The History of the Department of Homeland Security System of Records is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to the enforcement of civil and criminal laws; investigations, inquiries, and proceedings thereunder; national security and intelligence activities; and protection of the President of the United States or other individuals pursuant to section 3056 and 3056A of Title 18. The DHS/ALL—027 The History of the Department of Homeland Security System of Records contain information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other federal, state, local, tribal, foreign, or international government agencies. The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to limitations set forth in 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8), (e)(12); (f); (g)(1); and (h) pursuant to 5 U.S.C. 552a(j)(2). Additionally, the Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to limitations set forth in 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f) pursuant to 5 U.S.C. 552a(k)(1), (k)(2), (k)(3), and (k)(5). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS or another agency. Access to the

records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continually re-investigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced occasionally may be unclear, or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of the investigation, thereby interfering with that investigation and related law enforcement activities.

(e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information could impede law enforcement by compromising the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(f) From subsections (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements) and (f) (Agency Rules), because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

(g) From subsection (e)(5) (Collection of Information) because with the collection of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with subsection (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.

(h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere

with DHS's ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal and could result in disclosure of investigative techniques, procedures, and evidence.

(i) From subsection (e)(12) (Computer Matching) if the agency is a recipient agency or a source agency in a matching program with a non-Federal agency, with respect to any establishment or revision of a matching program, at least 30 days prior to conducting such program, publish in the FEDERAL REGISTER notice of such establishment or revision.

(j) From subsection (g)(1) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act.

(k) From subsection (h) (Legal Guardians) the parent of any minor, or the legal guardian of any individual who has been declared to be incompetent due to physical or mental incapacity or age by a court of competent jurisdiction, may act on behalf of the individual.

52. The DHS/ALL—031 ISE SAR Initiative System of Records consists of electronic records and will be used by DHS and its components. The DHS/ALL—031 ISE SAR Initiative System of Records is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to the enforcement of civil and criminal laws; investigations, inquiries, and proceedings there under; national security and intelligence activities; and protection of the President of the U.S. or other individuals pursuant to Section 3056 and 3056A of Title 18. The DHS/ALL—031 ISE SAR Initiative System of Records contains information that is collected by, on behalf of, in support of, or in cooperation with DHS, its components, as well as other federal, state, local, tribal, or foreign agencies or private sector organization and may contain personally identifiable information collected by other federal, state, local, tribal, foreign, or international government agencies. The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8), and (e)(12); (f); (g)(1); and (h) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2). Additionally, the Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitation set forth in 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(2) and (k)(3). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (c)(4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continually re-investigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced occasionally may be unclear, or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of the investigation, thereby interfering with that investigation and related law enforcement activities.

(e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information could impede law enforcement by compromising the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(f) From subsections (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements) and (f) (Agency Rules), because portions of this sys-

tem are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

(g) From subsection (e)(5) (Collection of Information) because with the collection of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with subsection (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.

(h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS's ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal and could result in disclosure of investigative techniques, procedures, and evidence.

(i) From subsection (e)(12) (Computer Matching) if the agency is a recipient agency or a source agency in a matching program with a non-Federal agency, with respect to any establishment or revision of a matching program, at least 30 days prior to conducting such program, publish in the FEDERAL REGISTER notice of such establishment or revision.

(j) From subsection (g)(1) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act.

(k) From subsection (h) (Legal Guardians) the parent of any minor, or the legal guardian of any individual who has been declared to be incompetent due to physical or mental incapacity or age by a court of competent jurisdiction, may act on behalf of the individual.

53. The DHS/USCIS-012 CIDR System of Records consists of electronic and paper records and will be used by DHS and its components. The DHS/USCIS-012 CIDR System of Records is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to the enforcement of civil and criminal laws; investigations, inquiries, and proceedings thereunder; national security and intelligence activities; and protection of the President of the U.S. or other individuals pursuant to Section 3056 and 3056A of Title 18. The DHS/USCIS-012 CIDR System of Records contains information that is collected by, on behalf of, in support of, or in

cooperation with DHS and its components and may contain PII collected by other federal, state, local, tribal, foreign, or international government agencies. The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to limitations set forth in 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f) pursuant to 5 U.S.C. 552a (k)(1) and (k)(2). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation, and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting could also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, to the existence of the investigation, and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an impossible administrative burden by requiring investigations to be continuously re-investigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced occasionally may be unclear or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsections (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements), and (f) (Agency Rules) because portions of this system are exempt from the individual access

provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

54. The DHS/USCG—008 Courts Martial Case Files System of Records consists of electronic and paper records and will be used by DHS/USCG. The DHS/USCG—008 Courts Martial Case Files System of Records is a repository of information held by DHS/USCG in connection with its several and varied missions and functions, including, but not limited to: the enforcement of civil and criminal laws; investigations, inquiries, and proceedings thereunder; and national security and intelligence activities. The DHS/USCG—008 Courts Martial Case Files System of Records contains information that is collected by, on behalf of, in support of, or in cooperation with DHS/USCG and may contain personally identifiable information collected by other federal, state, local, tribal, foreign, or international government agencies. The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(c)(3) and (c)(4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5) and (e)(8); (f); and (g) pursuant to 5 U.S.C. 552a(j)(2). Additionally, the Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f) pursuant to 5 U.S.C. 552a(k)(1) and (k)(2). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (c)(4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation, and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, to the existence of the investigation, and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an impossible administrative burden by requiring investigations to be continuously re-investigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced occasionally may be unclear or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of an investigation, thereby interfering with the related investigation and law enforcement activities.

(e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information would impede law enforcement in that it could compromise investigations by revealing the existence of an otherwise confidential investigation and thereby provide an opportunity for the subject of an investigation to conceal evidence, alter patterns of behavior, or take other actions that could thwart investigative efforts; reveal the identity of witnesses in investigations, thereby providing an opportunity for the subjects of the investigations or others to harass, intimidate, or otherwise interfere with the collection of evidence or other information from such witnesses; or reveal the identity of confidential informants, which would negatively affect the informant's usefulness in any ongoing or future investigations and discourage members of the public from cooperating as confidential informants in any future investigations.

(f) From subsections (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements), and (f) (Agency Rules) because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons

noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

(g) From subsection (e)(5) (Collection of Information) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.

(h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS' ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal, and could result in disclosure of investigative techniques, procedures, and evidence.

(i) From subsection (g) to the extent that the system is exempt from other specific subsections of the Privacy Act relating to individuals' rights to access and amend their records contained in the system. Therefore DHS is not required to establish rules or procedures pursuant to which individuals may seek a civil remedy for the agency's: refusal to amend a record; refusal to comply with a request for access to records; failure to maintain accurate, relevant, timely and complete records; or failure to otherwise comply with an individual's right to access or amend records.

55. The DHS/FEMA-011 Training and Exercise Program Records System of Records consists of electronic and paper records and will be used by FEMA. The DHS/FEMA-011 Training and Exercise Program Records System of Records consists of electronic and paper records and will be used by DHS and its components and offices to maintain records about individual training, including enrollment and participation information, information pertaining to class schedules, programs, and instructors, training trends and needs, testing and examination materials, and assessments of training efficacy. The data will be collected by employee name or other unique identifier. The collection and maintenance of this information will assist DHS in meeting its obligation to train its personnel and contractors in order to ensure that the agency mission can be successfully accomplished. The DHS/FEMA-011 General Training and Exercise Program Records System of Records contains information that is

collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other Federal, State, local, tribal, foreign, or international government agencies. The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to limitations set forth in 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f) pursuant to 5 U.S.C. 552a(k)(6) where it states: "For testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service the disclosure of which would compromise the objectivity or fairness of the testing or examination process."

Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continually re-investigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced occasionally may be unclear, or the information may not be strictly relevant or necessary to a specific

investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsections (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements) and (f) (Agency Rules), because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

56. The DHS/TSA-023 Workplace Violence Prevention Program System of Records consists of electronic and paper records and is used by the TSA in the administration of its Workplace Violence Prevention Program, an internal TSA program designed to prevent and respond to workplace violence. The DHS/TSA-023 Workplace Violence Prevention Program System of Records is a repository of information held by TSA in connection with its several and varied missions and functions, including, but not limited to: The enforcement of civil and criminal laws; investigations, inquiries, and proceedings there under. The DHS/TSA-023 Workplace Violence Prevention Program System of Records contains information collected by TSA, and may contain personally identifiable information collected by other federal, state, local, tribal, foreign, or international government agencies. The Secretary of Homeland Security has exempted portions of this system from the following provisions of the Privacy Act, subject to the limitations set forth in (c)(3); (d); (e)(1), (e)(4)(G); (e)(4)(H); (e)(4)(I); and (f) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(2). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid

detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continually re-investigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced occasionally may be unclear, or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsections (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements) and (f) (Agency Rules), because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

57. The DHS/OPS–002 National Operations Center Tracker and Senior Watch Officer Logs Records System of Records consists of electronic and paper records and will be used by DHS and its components. The DHS/OPS–002 National Operations Center Tracker and Senior Watch Officer Logs Records System of Records is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to the enforcement of civil and criminal laws; investigations, inquiries, and proceedings there under; national security and intelligence activities; and protection of the President of the U.S. or other individuals pursuant to Section 3056 and 3056A

of Title 18. The DHS/OPS–002 National Operations Center Tracker and Senior Watch Officer Logs Records System of Records contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other federal, state, local, tribal, foreign, or international government agencies. The Secretary of Homeland Security is exempting this system from the following provisions of the Privacy Act, subject to limitations set forth in 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f) pursuant to 5 U.S.C. 552a(k)(1), (k)(2), and (k)(3). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continually re-investigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced occasionally may be unclear, or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain

all information that may aid in establishing patterns of unlawful activity.

(d) From subsections (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements) and (f) (Agency Rules), because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

59. The DHS/NPPD-001 NICC Records System of Records consists of electronic and paper records and will be used by DHS and its components. The DHS/NPPD-001 NICC Records System of Records is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to the enforcement of civil and criminal laws; investigations, inquiries, and proceedings there under; national security and intelligence activities. The DHS/NPPD-001 NICC Records System of Records contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other Federal, state, local, Tribal, foreign, or international government agencies. The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to limitations set forth in 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f) pursuant to 5 U.S.C. 552a(k)(1) and (k)(2). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in

this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continually re-investigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of Federal law, the accuracy of information obtained or introduced occasionally may be unclear, or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsections (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements) and (f) (Agency Rules), because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

64. The DHS/USCIS-015 Electronic Immigration System-2 Account and Case Management System of Records consists of electronic and paper records and will be used by DHS and its components. The DHS/USCIS-015 Electronic Immigration System-2 Account and Case Management is a repository of information held by USCIS to serve its mission of processing immigration benefits. This system also supports certain other DHS programs whose functions include, but are not limited to, the enforcement of civil and criminal laws; investigations, inquiries, and proceedings there under; and national security and intelligence activities. The DHS/USCIS-015 Electronic Immigration System-2 Account and Case Management System of Records contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components

and may contain personally identifiable information collected by other federal, state, local, Tribal, foreign, or international government agencies. This system is exempted from the following provisions of the Privacy Act pursuant to 5 U.S.C. 552a(k)(2); 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f). Additionally, many of the functions in this system require retrieving records from law enforcement systems. Where a record received from another system has been exempted in that source system under 5 U.S.C. 552a(j)(2), DHS will claim the same exemptions for those records that are claimed for the original primary systems of records from which they originated and claims any additional exemptions in accordance with this rule. Exemptions from these particular subsections are justified, on a case-by-case basis determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and/or reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continually re-investigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced occasionally may be unclear, or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective

law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsections (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements) and (f) (Agency Rules) because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records, or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system, would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

65. The DHS/USCIS-016 Electronic Immigration System-3 Automated Background Functions System of Records consists of electronic and paper records and will be used by DHS and its components. The DHS/USCIS-016 Electronic Immigration System-3 Automated Background Functions System of Records is a repository of information held by USCIS to serve its mission of processing immigration benefits. This system also supports certain other DHS programs whose functions include, but are not limited to, the enforcement of civil and criminal laws; investigations, inquiries, and proceedings there under; and national security and intelligence activities. The DHS/USCIS-016 Electronic Immigration System-3 Automated Background Functions System of Records contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other federal, state, local, Tribal, foreign, or international government agencies. This system is exempted from the following provisions of the Privacy Act pursuant to 5 U.S.C. 552a(k)(2); 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f). Additionally, many of the functions in this system require retrieving records from law enforcement systems. Where a record received from another system has been exempted in that source system under 5 U.S.C. 552a(j)(2), DHS will claim the same exemptions for those records that are claimed for the original primary systems of records from which they originated and claims any additional exemptions in accordance with this rule. Exemptions from these particular subsections are justified, on a case-by-case basis determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the

existence of that investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and/or reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continually re-investigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced occasionally may be unclear, or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsections (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements) and (f) (Agency Rules), because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records, or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system, would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

66. The DHS/ALL-030 Use of the Terrorist Screening Database System of Records consists of electronic and paper records and will be used by DHS and its Components. The DHS/ALL-030 Use of the Terrorist Screening Database System of Records is a repository

of information held by DHS in connection with its several and varied missions and functions, including, the enforcement of civil and criminal laws; investigations, inquiries, and proceedings thereunder; and national security and intelligence activities. The Terrorist Screening Database belongs to the Department of Justice (DOJ)/Federal Bureau of Investigation (FBI). DHS does not change or alter these records. All records within the DHS/ALL-030 Use of the Terrorist Screening Database System of Records are collected and disseminated by the DOJ/FBI and are covered by the DOJ/FBI-019, "Terrorist Screening Records Center System," 72 FR 77846 (Dec. 14, 2011). Because DHS does not make any changes to the records obtained from DOJ/FBI, the same exemptions outlined in the DOJ/FBI SORN, and reasons provided in its implementing regulations for use of such exemptions at 28 CFR 16.96, transfer and apply. The Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(j)(2), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3), (c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(5), (e)(8), and (g). When a record has been received from DOJ/FBI-019 Terrorist Screening Records System of Records and has been exempted in that source system, DHS will claim the same exemptions for those records that are claimed for that original primary system of records from which they originated and claims any additional exemptions set forth here. Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is

the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continually re-investigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of Federal law, the accuracy of information obtained or introduced occasionally may be unclear, or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of the investigation, thereby interfering with that investigation and related law enforcement activities.

(e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information could impede law enforcement by compromising the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(f) From subsection (e)(5) (Collection of Information) because with the collection of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with subsection (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.

(g) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS's ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal and could result in disclosure of investigative techniques, procedures, and evidence.

(h) From subsection (g) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act.

67. The DHS/FEMA–012 Suspicious Activity Reporting System of Records consists of electronic and paper records and will be used by DHS/FEMA and its components. The DHS/FEMA–012 Suspicious Activity Reporting System of Records is a repository of information held by DHS/FEMA to serve its mission to support our citizens and first responders to ensure that as a nation we work

together to build, sustain, and improve our capability to prepare for, protect against, respond to, recover from, and mitigate all hazards. This system also supports certain other DHS/FEMA programs whose functions include, but are not limited to, the enforcement of civil and criminal laws; investigations, inquiries, and proceedings there under; and national security and intelligence activities. The DHS/FEMA–012 Suspicious Activity Reporting System of Records contains information that is collected by, on behalf of, in support of, or in cooperation with DHS/FEMA and its components and may contain personally identifiable information collected by other federal, state, local, tribal, foreign, or international government agencies. The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act pursuant to 5 U.S.C. 552a(k)(2); (c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f). Exemptions from these particular subsections are justified, on a case-by-case basis determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS/FEMA as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS/FEMA or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continually re-investigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the

course of investigations into potential violations of federal law, the accuracy of information obtained or introduced occasionally may be unclear, or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsections (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements) and (f) (Agency Rules), because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS/FEMA is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

68. The DHS OPS-003 Operations Collection, Planning, Coordination, Reporting, Analysis, and Fusion System of Records consists of electronic and paper records and will be used by DHS and its components. The DHS OPS-003 Operations Collection, Planning, Coordination, Reporting, Analysis, and Fusion System of Records is a repository of information held by DHS to serve its several and varied missions and functions. This system also supports certain other DHS programs whose functions include, but are not limited to, the enforcement of civil and criminal laws; investigations, inquiries, and proceedings there under; national security and intelligence activities; and protection of the President of the U.S. or other individuals pursuant to Section 3056 and 3056A of Title 18. The DHS OPS-003 Operations Collection, Planning, Coordination, Reporting, Analysis, and Fusion System of Records contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other federal, state, local, tribal, foreign, or international government agencies. This system is exempted from the following provisions of the Privacy Act pursuant to 5 U.S.C. 552a(k)(1), (k)(2), (k)(3); 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal in-

vestigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access and Amendment) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continually reinvestigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced occasionally may be unclear, or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsections (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements) and (f) (Agency Rules), because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

69. The DHS/CBP-017 Analytical Framework for Intelligence (AFI) System of Records consists of electronic and paper records and will be used by DHS and its components. The DHS/CBP-017 Analytical Framework for Intelligence (AFI) System of

Records is a repository of information held by DHS to enhance DHS's ability to: Identify, apprehend, and/or prosecute individuals who pose a potential law enforcement or security risk; aid in the enforcement of the customs and immigration laws, and other laws enforced by DHS at the border; and enhance United States security. This system also supports certain other DHS programs whose functions include, but are not limited to, the enforcement of civil and criminal laws; investigations, inquiries, and proceedings there under; and national security and intelligence activities. The DHS/CBP—017 Analytical Framework for Intelligence (AFI) System of Records contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other federal, state, local, tribal, foreign, or international government agencies.

(a) The Secretary of Homeland Security has exempted this system from certain provisions of the Privacy Act as follows:

(1) Pursuant to 5 U.S.C. 552a(j)(2), the system is exempt from 5 U.S.C. 552a(c)(3) and (c)(4), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8), (f), and (g).

(2) Pursuant to 5 U.S.C. 552a(j)(2), the system (except for any records that were ingested by AFI where the source system of records already provides access and/or amendment under the Privacy Act) is exempt from 5 U.S.C. 552a(d)(1), (d)(2), (d)(3), and (d)(4).

(3) Pursuant to 5 U.S.C. 552a(k)(1), the system is exempt from 5 U.S.C. 552a(c)(3); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f).

(4) Pursuant to 5 U.S.C. 552a(k)(1), the system is exempt from (d)(1), (d)(2), (d)(3), and (d)(4).

(5) Pursuant to 5 U.S.C. 552a(k)(2), the system is exempt from 5 U.S.C. 552a(c)(3); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f).

(6) Pursuant to 5 U.S.C. 552a(k)(2), the system (except for any records that were ingested by AFI where the source system of records already provides access and/or amendment under the Privacy Act) is exempt from (d)(1), (d)(2), (d)(3), and (d)(4).

(b) Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(1) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting

would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(2) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continually re-investigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(3) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced occasionally may be unclear, or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement and national security, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(4) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of the investigation, thereby interfering with that investigation and related law enforcement and national security activities.

(5) From subsection (e)(3) (Notice to Individuals) because providing such detailed information could impede law enforcement and national security by compromising the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(6) From subsections (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements) and (f) (Agency Rules), because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to

themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

(7) From subsection (e)(5) (Collection of Information) because with the collection of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with subsection (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.

(8) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS's ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal and could result in disclosure of investigative techniques, procedures, and evidence.

(9) From subsection (g)(1) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act.

70. DHS/USCIS-ICE-CBP-001 Alien File, Index, and National File Tracking System of Records consists of electronic and paper records and will be used by USCIS, ICE, and CBP. DHS/USCIS-ICE-CBP-001 Alien File, Index, and National File Tracking System of Records is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to: The enforcement of civil and criminal laws; investigations, inquiries, and proceedings thereunder; and national security and intelligence activities. DHS/USCIS-ICE-CBP-001 Alien File, Index, and National File Tracking System of Records contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other federal, state, local, tribal, territorial, foreign, or international government agencies. The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2): 5 U.S.C. 552a(c)(3) and (c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8), (e)(12), (f), (g)(1), and (h). Additionally, the Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act pursuant to 5 U.S.C. 552a(k)(1) and (k)(2): 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f). Exemptions from these particular subsections may be justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory viola-

tion to the existence of that investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continually re-investigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced occasionally may be unclear, or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of the investigation, thereby interfering with that investigation and related law enforcement activities.

(e) From subsection (e)(3) (Notice to Individuals) because providing such detailed information could impede law enforcement by compromising the existence of a confidential investigation or reveal the identity of witnesses, DHS employees, or confidential informants.

(f) From subsections (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements) and (f) (Agency Rules), because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or

procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, potential witnesses, and confidential informants.

(g) From subsection (e)(5) (Collection of Information) because with the collection of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with subsection (e)(5) would impede DHS officials' ability to effectively use their investigative training and exercise good judgment to both conduct and report on investigations.

(h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS's ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal and could result in disclosure of investigative techniques, procedures, and evidence.

(i) From subsection (e)(12) (Computer Matching) if the agency is a recipient agency or a source agency in a matching program with a non-Federal agency, with respect to any establishment or revision of a matching program, at least 30 days prior to conducting such program, publish in the FEDERAL REGISTER notice of such establishment or revision.

(j) From subsection (g)(1) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act. (k) From subsection (h) (Legal Guardians) if the parent of any minor, or the legal guardian of any individual who has been declared to be incompetent due to physical or mental incapacity or age by a court of competent jurisdiction, is acting on behalf of the individual.

71. The Department of Homeland Security (DHS)/Transportation Security Administration (TSA)-021 TSA Pre✓™ Application Program System of Records consists of electronic and paper records and will be used by DHS/TSA. The DHS/TSA-021 Pre✓™ Application Program System of Records is a repository of information held by DHS/TSA on individuals who voluntarily provide personally identifiable information (PII) to TSA in return for enrollment in a program that will make them eligible for expedited security screening at designated airports. This System of Records contains PII in biographic application data, biometric information, pointer information to law enforcement databases, payment tracking, and U.S. application membership decisions that support the TSA Pre✓™ Application Program membership decisions. The DHS/TSA-021 TSA

Pre✓™ Application Program System of Records contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain PII collected by other federal, state, local, tribal, territorial, or foreign government agencies. The Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(k)(1) and (k)(2), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3); (d); (e)(1); (e)(4)(G), (H), and (I); and (f). Where a record received from another system has been exempted in that source system under 5 U.S.C. 552a(k)(1) and (k)(2), DHS will claim the same exemptions for those records that are claimed for the original primary systems of records from which they originated and claims any additional exemptions set forth here. Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting also would permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continually re-investigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced occasionally may be unclear, or the information may not

be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsections (e)(4)(G), (H), and (I) (Agency Requirements) and (f) (Agency Rules), because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to the existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, potential witnesses, and confidential informants.

72. The DHS/ICE-014 Homeland Security Investigations Forensic Laboratory System of Records consists of electronic and paper records that will be used by DHS and its components. The DHS/ICE-014 Homeland Security Investigations Forensic Laboratory System of Records contains records of evidence and cases submitted to the HSI-FL. This information will include information on the individual submitting the request, identify the evidence submitted, track the evidence as it moves throughout the HSI-FL, capture case notes and results of examinations, store electronic images of evidence, and produce reports of findings. Other case-related records are maintained, including descriptions of expert witness testimony provided by HSI-FL employees. Records in the DHS/ICE-014 Homeland Security Investigations Forensic Laboratory System of Records also include the library of genuine, altered, and counterfeit travel and identity documents provided to the HSI-FL by international organizations, government agencies, and law enforcement organizations from across the United States and around the world to research methods of document production and authenticate documents through comparative forensic examinations. The DHS/ICE-014 Homeland Security Investigations Forensic Laboratory System of Records contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components, and may contain personally identifiable information (PII) collected by other federal, state, local, tribal, foreign, or international government agencies. The Secretary of the Department of Homeland Security, pursuant to 5 U.S.C. 552a(j)(2), has exempted this system from the following provisions of the Privacy Act, subject to limitations set forth in 5 U.S.C. 552a(c)(3), (c)(4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8); (f); and (g). Additionally, the Sec-

retary of Homeland Security, pursuant to 5 U.S.C. 552a(k)(2), has exempted this system from the following provisions of the Privacy Act, subject to limitations set forth in 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f). Where a record received from another system has been exempted in that source system under 5 U.S.C. 552a(j)(2), DHS will claim the same exemptions for those records that are claimed for the original primary systems of records from which they originated and claims any additional exemptions set forth here. Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continually re-investigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced occasionally may be unclear, or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of the investigation, thereby interfering with that investigation and related law enforcement activities.

(e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information could impede law enforcement by compromising the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(f) From subsections (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements) and (f) (Agency Rules), because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

(g) From subsection (e)(5) (Collection of Information) because with the collection of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with subsection (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.

(h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS's ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal and could result in disclosure of investigative techniques, procedures, and evidence.

(i) From subsection (g)(1) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act.

73. The DHS/NPPD—002 Chemical Facility Anti-Terrorism Standards Personnel Surety Program System of Records consists of electronic and paper records and will be used by DHS and its components. The DHS/NPPD—002 Chemical Facility Anti-Terrorism Standards Personnel Surety Program System of Records is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to the enforcement of civil and criminal laws; investigations, inquiries, and proceedings thereunder; and national security and intelligence activities. The DHS/NPPD—002 Chemical Facility Anti-Ter-

rorism Standards Personnel Surety Program System of Records contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other federal, state, local, tribal, foreign, or international government agencies. The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to limitations set forth therein: 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f). These exemptions are made pursuant to 5 U.S.C. 552a(k)(1) and (k)(2).

In addition to records under the control of DHS, the DHS/NPPD—002 Chemical Facility Anti-Terrorism Standards Personnel Surety Program System of Records may include records originating from systems of records of other law enforcement and intelligence agencies, which may be exempt from certain provisions of the Privacy Act. DHS does not, however, assert exemption from any provisions of the Privacy Act with respect to information submitted by high-risk chemical facilities.

To the extent the DHS/NPPD—002 Chemical Facility Anti-Terrorism Standards Personnel Surety Program System of Records contains records originating from other systems of records, DHS will rely on the exemptions claimed for those records in the originating systems of records. Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest, on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is

the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continually re-investigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced occasionally may be unclear, or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsections (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements) and (f) (Agency Rules), because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, potential witnesses, and confidential informants.

74. The DHS/CBP-022 Electronic Visa Update System (EVUS) System of Records consists of electronic and paper records and will be used by DHS and its components. EVUS is a repository of information held by DHS/CBP in connection with its several and varied missions and functions, including, but not limited to the enforcement of civil and criminal laws; investigations, inquiries, and proceedings there under; and national security and intelligence activities. EVUS contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other federal, state, local, tribal, foreign, or international government agencies. The Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(j)(2), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3), (e)(8), and (g). Additionally, the Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(k)(2) has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3). Exemptions from these particular subsections are justified, on a case-by-case basis

to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS's ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal and could result in disclosure of investigative techniques, procedures, and evidence.

(c) From subsection (g) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act.

75. The DHS/ICE-015 LeadTrac System of Records consists of electronic and paper records and will be used by ICE investigative and homeland security personnel. The DHS/ICE-015 LeadTrac System of Records is a repository of information held by ICE for analytical and investigative purposes. The system is used to conduct research supporting the production of law enforcement activities; provide lead information for investigative inquiry and follow-up; assist in the conduct of ICE criminal and administrative investigations; assist in the disruption of terrorist or other criminal activity; and discover previously unknown connections among existing ICE investigations. The DHS/ICE-015 LeadTrac System of Records contains aggregated data from ICE and DHS law enforcement and homeland security IT systems, as well as data uploaded by ICE personnel for analysis from various public, private, and commercial sources during the course of an investigation or analytical project. The Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(j)(2), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3), (c)(4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8); (f); and (g). Additionally, the Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(k)(2), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3), (c)(4); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f). When a record received from another system has been exempted in that source system under 5 U.S.C. 552a(j)(2) or (k)(2), DHS will claim the

same exemptions for those records that are claimed for the original primary systems of records from which they originated and claims any additional exemptions set forth here.

Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process. Disclosure of corrections or notations of dispute may impede investigations by requiring DHS to inform each witness or individual contacted during the investigation of each correction or notation pertaining to information provided them during the investigation.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continually re-investigated. In addition, permitting access and amendment to such information could disclose classified and other security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced occasionally may be unclear, or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of the investigation, thereby interfering with that investigation and related law enforcement activities.

(e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information could impede law enforcement by compromising the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(f) From subsections (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements) and (f) (Agency Rules), because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise establishing procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, potential witnesses, and confidential informants.

(g) From subsection (e)(5) (Collection of Information) because with the collection of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with subsection (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.

(h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS's ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal and could result in disclosure of investigative techniques, procedures, and evidence.

(i) From subsection (g)(1) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act.

76. The DHS/CBP-023 Border Patrol Enforcement Records (BPER) System of Records consists of electronic and paper records and will be used by DHS and its components. The DHS/CBP-023 BPER System of Records is a repository of information held by DHS/CBP in connection with its several and varied missions and functions, including, but not limited to the enforcement of civil and criminal laws; investigations, inquiries, and proceedings there under; and national security and intelligence activities. The DHS/CBP-023 BPER System of Records contains information that is collected by, on behalf of, in support of, or in cooperation with

DHS and its components and may contain personally identifiable information collected by other federal, state, local, tribal, foreign, or international government agencies. The Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(j)(2), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. 552a (c)(3), (c)(4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(5), (e)(8); and (g). Additionally, the Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(k)(2), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. 552a (c)(3); (d); (e)(1), (e)(4)(G), and (e)(4)(H). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continually re-investigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced occasionally may be unclear, or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain

all information that may aid in establishing patterns of unlawful activity.

(d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of the investigation, thereby interfering with that investigation and related law enforcement activities.

(e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information could impede law enforcement by compromising the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(f) From subsections (e)(4)(G) and (e)(4)(H) (Agency Requirements) because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

(g) From subsection (e)(5) (Collection of Information) because with the collection of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with subsection (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.

(h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS's ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal and could result in disclosure of investigative techniques, procedures, and evidence.

(i) From subsection (g)(1) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act.

77. The DHS/USCG-031 USCG Law Enforcement (ULE) System of Records consists of electronic and paper records and will be used by DHS and its components. The DHS/USCG-031 USCG Law Enforcement (ULE) System of Records is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to the enforcement of civil and criminal laws; investigations, inquiries, and proceedings there under; and national security and intelligence activities. The DHS/USCG-031 USCG Law Enforcement (ULE) System of Records contains information that

is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other federal, state, local, tribal, foreign, or international government agencies. The Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(j)(2), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. 552a (c)(3–4); (d); (e)(1–3), (e)(5), (e)(8); and (g). Additionally, the Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(k)(2) has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. 552a (c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f). When a record received from another system has been exempted in that source system under 5 U.S.C. 552a(j)(2), DHS will claim the same exemptions for those records that are claimed for the original primary systems of records from which they originated and claims any additional exemptions set forth here.

Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continually re-investigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced occasionally may be unclear, or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of the investigation, thereby interfering with that investigation and related law enforcement activities.

(e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information could impede law enforcement by compromising the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(f) From subsection (e)(5) (Collection of Information) because with the collection of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with subsection (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.

(g) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS's ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal and could result in disclosure of investigative techniques, procedures, and evidence.

(h) From subsection (g) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act.

78. The DHS/ALL-039 Foreign Access Management System of Records consists of electronic and paper records and will be used by DHS and its components. The DHS/ALL-039 Foreign Access Management System of Records is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to the enforcement of civil and criminal laws; investigations, inquiries, and proceedings there under; and national security and intelligence activities. The DHS/ALL-039 Foreign Access Management System of Records contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other federal, state, local, tribal, foreign, or international government agencies. The Secretary of Homeland Security, pursuant to 5 U.S.C.

552a(k)(1), (k)(2), and (k)(5), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f). When a record received from another system has been exempted in that source system under 5 U.S.C. 552a(j)(2), DHS will claim the same exemptions for those records that are claimed for the original primary systems of records from which they originated and claims any additional exemptions set forth here. Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process. When an investigation has been completed, information on disclosures made may continue to be exempted if the fact that an investigation occurred remains sensitive after completion.

(b) From subsection (d) (Access and Amendment to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continually reinvestigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced occasionally may be unclear, or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective

law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsections (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements) and (f) (Agency Rules), because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses and potential witnesses, and confidential informants.

79. The DHS/CBP-024 CBP Intelligence Records System (CIRS) System of Records consists of electronic and paper records and will be used by DHS and its components. The CIRS is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to the enforcement of civil and criminal laws; investigations, inquiries, and proceedings there under; and national security and intelligence activities. The CIRS contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other Federal, state, local, tribal, foreign, or international government agencies. The Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(j)(2), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I); (e)(5), and (e)(8); (f); and (g). Additionally, the Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(k)(1) and (k)(2), has exempted this system from the following provisions of the Privacy Act, 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f). When this system receives a record from another system exempted in that source system under 5 U.S.C. 552a(k)(1), (k)(2), or (j)(2), DHS will claim the same exemptions for those records that are claimed for the original primary systems of records from which they originated and claims any additional exemptions set forth here. Exemptions from these particular subsections are justified, on a case by case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part

of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process. Information on a completed investigation may be withheld and exempt from disclosure if the fact that an investigation occurred remains sensitive after completion.

(b) From subsection (d) (Access and Amendment to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continually reinvestigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of Federal law, the accuracy of information obtained or introduced occasionally may be unclear, or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of the investigation, thereby interfering with that investigation and related law enforcement activities.

(e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information could impede law enforcement by compromising the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(f) From subsections (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements) and (f) (Agency Rules) because portions of this system are exempt from the individual access and amendment provisions of subsection (d)

for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access, amend, and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

(g) From subsection (e)(5) (Collection of Information) because with the collection of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with subsection (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.

(h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS's ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal and could result in disclosure of investigative techniques, procedures, and evidence.

(i) From subsection (g) to the extent that the system is exempt from other specific subsections of the Privacy Act relating to individuals' rights to access and amend their records contained in the system. Therefore, DHS is not required to establish rules or procedures pursuant to which individuals may seek a civil remedy for the agency's refusal to amend a record, refusal to comply with a request for access to records, failure to maintain accurate, relevant timely and complete records, or its failure to otherwise comply with an individual's right to access or amend records.

80. The DHS/ICE-007 Criminal History and Immigration Verification (CHIVE) System of Records consists of electronic and paper records and will be used by DHS and its components. The CHIVE System of Records is a repository of information held by DHS in connection with its several and varied missions and functions, including the enforcement of civil and criminal laws; investigations, inquiries, and proceedings thereunder; and national security and intelligence activities. The CHIVE System of Records contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other federal, state, local, tribal, foreign, or international government agencies. The Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(j)(2), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3) and (c)(4); (d); (e)(1),

(e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8); (f); and (g). Additionally, the Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(k)(2), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H); and (f). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process. Information on a completed investigation may be withheld and exempt from disclosure if the fact that an investigation occurred remains sensitive after completion.

(b) From subsection (d) (Access and Amendment to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continually reinvestigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced occasionally may be unclear, or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsection (e)(2) (Collection of Information from Individuals) because requir-

ing that information be collected from the subject of an investigation would alert the subject to the nature or existence of the investigation, thereby interfering with that investigation and related law enforcement activities.

(e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information could impede law enforcement by compromising the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(f) From subsections (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements) and (f) (Agency Rules), because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

(g) From subsection (e)(5) (Collection of Information) because with the collection of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with subsection (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.

(h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS's ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal and could result in disclosure of investigative techniques, procedures, and evidence.

(j) From subsection (g) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act.

81. The DHS/ICE-016 FALCON Search and Analysis (FALCON-SA) System of Records consists of electronic and paper records and will be used by DHS and its components. The FALCON-SA System of Records is a repository of information held by DHS in connection with its several and varied missions and functions, including the enforcement of civil and criminal laws; investigations, inquiries, and proceedings thereunder; and national security and intelligence activities. The FALCON-SA System of Records contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other

federal, state, local, tribal, foreign, or international government agencies. The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to limitations set forth in 5 U.S.C. 552a(c)(3) and (c)(4): (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8); (f); and (g) pursuant to 5 U.S.C. 552a(j)(2). Additionally, the Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to limitations set forth in 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f) pursuant to 5 U.S.C. 552a(k)(2). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process. Information on a completed investigation may be withheld and exempt from disclosure if the fact that an investigation occurred remains sensitive after completion.

(b) From subsection (d) (Access and Amendment to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continually reinvestigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of federal law, the accuracy of informa-

tion obtained or introduced occasionally may be unclear, or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of the investigation, thereby interfering with that investigation and related law enforcement activities.

(e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information could impede law enforcement by compromising the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(f) From subsections (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements) and (f) (Agency Rules), because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

(g) From subsection (e)(5) (Collection of Information) because with the collection of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with subsection (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.

(h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS's ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal and could result in disclosure of investigative techniques, procedures, and evidence.

(j) From subsection (g) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act.

[71 FR 20523, Apr. 21, 2006]

EDITORIAL NOTE: For FEDERAL REGISTER citations affecting appendix C to part 5, see the List of CFR Sections Affected, which appears in the Finding Aids section of the printed volume and at [www.govinfo.gov](http://www.govinfo.gov).

## PART 7—CLASSIFIED NATIONAL SECURITY INFORMATION

### Sec.

- 7.1 Purpose.
- 7.2 Scope.
- 7.3 Definitions.

#### Subpart A—Administration

- 7.10 Authority of the DHS Chief Security Officer.
- 7.11 Components' responsibilities.
- 7.12 Violations of classified information requirements.
- 7.13 Judicial proceedings.

#### Subpart B—Classified Information

- 7.20 Classification and declassification authority.
- 7.21 Classification of information, limitations.
- 7.22 Classification pending review.
- 7.23 Emergency release of classified information.
- 7.24 Duration of classification.
- 7.25 Identification and markings.
- 7.26 Derivative classification.
- 7.27 Declassification and downgrading.
- 7.28 Automatic declassification.
- 7.29 National Declassification Center.
- 7.30 Documents of permanent historical value.
- 7.31 Classification challenges.
- 7.32 Mandatory declassification review.

AUTHORITY: 5 U.S.C. 301; Pub. L. 107-296; E.O. 13526; 3 CFR, 1995 Comp., p. 333; E.O. 13142, 64 FR 66089, 3 CFR, 1999 Comp., p. 236; 32 CFR part 2001.

SOURCE: 79 FR 44095, July 30, 2014, unless otherwise noted.

#### § 7.1 Purpose.

The purpose of this part is to ensure that information within the Department of Homeland Security (DHS) relating to the national security is classified, safeguarded, and declassified pursuant to the provisions of Executive Order 13526, and implementing directives from the Information Security Oversight Office (ISOO) of the National Archives and Records Administration (NARA).

#### § 7.2 Scope.

(a) This part applies to all employees, detailees, and non-contractor personnel inside and outside the Executive Branch who are granted access to classified information by the DHS, in accordance with the standards in Execu-

tive Order 13526, and its implementing directives, and Executive Order 13549, "Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities," and its implementing directives.

(b) This part does not apply to contractors, grantees and other categories of personnel falling under the purview of Executive Order 12829, National Industrial Security Program, as amended, and its implementing directives.

(c) This part is independent of and does not affect any classification procedures or requirements of the Atomic Energy Act of 1954, as amended (42 U.S.C. 2011 *et seq.*).

(d) This part does not, and is not intended to, create any right to judicial review, or any other right or benefit or trust responsibility, substantive or procedural, enforceable by a party against the United States, its agencies or instrumentalities, its officers or employees, or any other person. This part creates limited rights to administrative review of decisions. This part does not, and is not intended to, create any right to judicial review of administrative action.

#### § 7.3 Definitions.

The terms defined or used in Executive Order 13526, and the implementing directives in 32 CFR part 2001 and 2004 are applicable to this part.

#### Subpart A—Administration

#### § 7.10 Authority of the DHS Chief Security Officer.

(a) The DHS Chief Security Officer (hereafter "Chief Security Officer") is designated as the Senior Agency Official as required by section 5.4(d) of Executive Order 13526, and, except as specifically provided elsewhere in this part, is authorized to administer the DHS Classified National Security Information program pursuant to Executive Order 13526.

(b) To the extent that 32 CFR part 2001 refers to the agency head or "designee," the Chief Security Officer is such designee unless determined otherwise by the Secretary. The Chief Security Officer may further delegate the associated authorities.