

## Pt. 5, App. C

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, Glynnco, 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).

## 6 CFR Ch. I (1-1-19 Edition)

### 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:

**Office of the Secretary, Homeland Security****Pt. 5, App. C**

(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

## Pt. 5, App. C

## 6 CFR Ch. I (1-1-19 Edition)

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.

**Office of the Secretary, Homeland Security****Pt. 5, App. C**

(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 reinvigorated 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

## Pt. 5, App. C

## 6 CFR Ch. I (1-1-19 Edition)

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

## Pt. 5, App. C

## 6 CFR Ch. I (1-1-19 Edition)

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 investigation, 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

## Pt. 5, App. C

## 6 CFR Ch. I (1-1-19 Edition)

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. 552a(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

## Pt. 5, App. C

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

## 6 CFR Ch. I (1-1-19 Edition)

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

**Office of the Secretary, Homeland Security****Pt. 5, App. C**

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

## Pt. 5, App. C

## 6 CFR Ch. I (1-1-19 Edition)

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 text 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. 5195cc(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

## Pt. 5, App. C

## 6 CFR Ch. I (1-1-19 Edition)

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 reinvigorated. 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

## Pt. 5, App. C

## 6 CFR Ch. I (1-1-19 Edition)

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

## Pt. 5, App. C

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,

## 6 CFR Ch. I (1-1-19 Edition)

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

**Office of the Secretary, Homeland Security****Pt. 5, App. C**

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 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 investigation 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.

## Pt. 5, App. C

(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

## 6 CFR Ch. I (1-1-19 Edition)

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. The DHS/ALL—018 Grievances, Appeals and Disciplinary Action Records system of records consists of electronic and paper records and will be used by DHS and its components. The DHS/ALL—018 Grievances, Appeals and Disciplinary Action 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; 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—018 Grievances, Appeals and Disciplinary Action 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 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.

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

## Pt. 5, App. C

## 6 CFR Ch. I (1-1-19 Edition)

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 viola-

tion 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

**Office of the Secretary, Homeland Security****Pt. 5, App. C**

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

## Pt. 5, App. C

## 6 CFR Ch. I (1-1-19 Edition)

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 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—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

**Office of the Secretary, Homeland Security****Pt. 5, App. C**

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

## Pt. 5, App. C

## 6 CFR Ch. I (1-1-19 Edition)

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 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

**Office of the Secretary, Homeland Security****Pt. 5, App. C**

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 Television system of records consists of electronic 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

## Pt. 5, App. C

## 6 CFR Ch. I (1-1-19 Edition)

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 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

**Office of the Secretary, Homeland Security****Pt. 5, App. C**

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 compo-

nents' 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

## Pt. 5, App. C

## 6 CFR Ch. I (1-1-19 Edition)

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. 552(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. (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

## Pt. 5, App. C

## 6 CFR Ch. I (1-1-19 Edition)

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

## Pt. 5, App. C

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.

## 6 CFR Ch. I (1-1-19 Edition)

(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

**Office of the Secretary, Homeland Security****Pt. 5, App. C**

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 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

## Pt. 5, App. C

## 6 CFR Ch. I (1-1-19 Edition)

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 terminations involving benefit fraud, crimi-

nal 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 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) and (e)(4)(H) (Agency Requirements) because portions of this system are exempt from the individual

**Office of the Secretary, Homeland Security****Pt. 5, App. C**

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

## Pt. 5, App. C

## 6 CFR Ch. I (1-1-19 Edition)

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

**Office of the Secretary, Homeland Security****Pt. 5, App. C**

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 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 individuals 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

## Pt. 5, App. C

## 6 CFR Ch. I (1-1-19 Edition)

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 pro-

viding 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 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, 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

## Pt. 5, App. C

## 6 CFR Ch. I (1-1-19 Edition)

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:

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 viola-

tion 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

## Pt. 5, App. C

## 6 CFR Ch. I (1-1-19 Edition)

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 lim-

ited 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

**Office of the Secretary, Homeland Security****Pt. 5, App. C**

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 sys-

tem 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/US-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

## **Office of the Secretary, Homeland Security**

## **Pt. 5, App. C**

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,

## Pt. 5, App. C

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.

## 6 CFR Ch. I (1-1-19 Edition)

(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

**Office of the Secretary, Homeland Security****Pt. 5, App. C**

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 wants or warrants, information from other government agencies regarding high-risk parties, and risk-based rules developed by analysts using law enforcement data, intelligence,

## Pt. 5, App. C

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

## 6 CFR Ch. I (1-1-19 Edition)

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 potential 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

## Pt. 5, App. C

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 (e)(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.

## 6 CFR Ch. I (1-1-19 Edition)

(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

## Office of the Secretary, Homeland Security

## Pt. 5, App. C

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

## Pt. 5, App. C

## 6 CFR Ch. I (1-1-19 Edition)

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:

**Office of the Secretary, Homeland Security****Pt. 5, App. C**

(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

## Pt. 5, App. C

## 6 CFR Ch. I (1-1-19 Edition)

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),

## Pt. 5, App. C

## 6 CFR Ch. I (1-1-19 Edition)

(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 in-

vestigation, 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 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

## Pt. 5, App. C

## 6 CFR Ch. I (1-1-19 Edition)

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 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

## Pt. 5, App. C

## 6 CFR Ch. I (1-1-19 Edition)

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

## Office of the Secretary, Homeland Security

## Pt. 5, App. C

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

## Pt. 5, App. C

## 6 CFR Ch. I (1-1-19 Edition)

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 inter-

fere 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:

## Pt. 5, App. C

## 6 CFR Ch. I (1-1-19 Edition)

(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 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 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

**Office of the Secretary, Homeland Security****Pt. 5, App. C**

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

## Pt. 5, App. C

## 6 CFR Ch. I (1-1-19 Edition)

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 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 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

## Pt. 5, App. C

## 6 CFR Ch. I (1-1-19 Edition)

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 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, 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-Terrorism 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

## Pt. 5, App. C

## 6 CFR Ch. I (1-1-19 Edition)

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

## Office of the Secretary, Homeland Security

## Pt. 5, App. C

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

## Pt. 5, App. C

## 6 CFR Ch. I (1-1-19 Edition)

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 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 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,

**Office of the Secretary, Homeland Security****Pt. 5, App. C**

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

## Pt. 5, App. C

## 6 CFR Ch. I (1-1-19 Edition)

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 inves-

tigative 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

## Pt. 7

## 6 CFR Ch. I (1-1-19 Edition)

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.

[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 Executive 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.