4410-10

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2014-0019]

Privacy Act of 1974; Department of Homeland Security – DHS/ALL 020 Internal Affairs System of Records.

AGENCY: Department of Homeland Security; Privacy Office.

ACTION: Notice of Privacy Act System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security proposes to update and reissue a current Department of Homeland Security department-wide system of records notice titled "Department of Homeland Security/ALL-020 Department of Homeland Security Internal Affairs System of Records." This system collects and maintains records relating to investigations, including allegations of misconduct, resultant investigations conducted by Department of Homeland Security (DHS) Headquarters or its components, and any of the individuals involved in such investigations with the exception of records of investigations conducted by the Office of the Inspector General. This revised notice includes several changes necessitated by the issuance of a final rule entitled Standards to Prevent, Detect, and Respond to Sexual Abuse and Assault in Confinement Facilities (6 CFR part 115) and to better reflect the DHS's internal affairs records systems, including changes to: (1) The categories of individuals first, by removing applicants for DHS employment and second, by adding any individual who is subject to or involved in an internal integrity or disciplinary inquiry, or an internal review, inspection, or investigation not handled by the

DHS Office of the Inspector General (OIG); (2) the categories of records, by adding two new categories; (3) the purpose of the system, by adding internal integrity or disciplinary inquiries, and internal reviews, inspections, or investigations DHS Headquarters or its components conduct, except any of the above that the DHS OIG conducts; (4) the routine uses, by adding new routine uses (K), (O), (P), (Q), (R), (S), (T), (U), and (V), and (5) the retention periods, by adding new retention periods for review files and sexual abuse and assault files. In addition, this notice includes non-substantive changes to simplify the formatting and text of the previously published notice. The exemptions claimed in this system of records notice also reflect updates necessary for consistency with the Final Rule for Privacy Act Exemptions, 74 Fed. Reg. 42575 (Aug. 24, 2009). This system is still included in the Department of Homeland Security's inventory of record systems. In addition to the changes above, this notice communicates DHS's intention to retire a different system of records from its inventory, because the Transportation Security Administration no longer requires the DHS/TSA 005 Internal Investigation Record System, 69 Fed Reg. 71828 (Dec. 10, 2004).

DATES: Submit comments on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. This new system will be effective [INSERT DATE 30 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: You may submit comments, identified by docket number DHS-2013-XXXX by one of the following methods:

- Federal e-Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.
- Fax: 202-343-4010.

- Mail: Karen L. Neuman, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.
- Instructions: All submissions received must include the agency name and docket number for this rulemaking. All comments received will be posted without change and may be read at http://www.regulations.gov, including any personal information provided.
- Docket: For access to the docket to read background documents or comments received, go to http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: For general questions and privacy issues please contact: Karen L. Neuman (202) 343-1717, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, the Department of Homeland Security (DHS) proposes to update and reissue the current DHS system of records titled, "DHS/ALL-020 Department of Homeland Security Internal Affairs System of Records," last published at 73 FR 221 (Nov. 14, 2008). The existing Internal Affairs System of Records Notice specifies that DHS collects and maintains records of applicants, past and present employees, contractors, and contractor applicants relating to investigations conducted by DHS Headquarters or its components—with the exception of investigations conducted by the OIG that are covered by DHS/OIG-002 Investigations Data Management System of Records.

In addition, this update will provide notice that DHS intends to retire a different system of records from its inventory because the Transportation Security Administration (TSA) no longer requires the system. The system DHS is retiring is DHS/TSA 005 Internal Investigation Record System, 69 FR 71828 (Dec. 10, 2004).

To better reflect the Department's internal affairs records system and to support the issuance of the final rule entitled Standards to Prevent, Detect, and Respond to Sexual Abuse and Assault in Confinement Facilities (6 CFR Part 115), 79 FR 13100 (Mar. 7, 2014), , DHS is updating the Department of Homeland Security Internal Affairs System of Records Notice to add a new category of individuals, new categories of records, an additional purpose for the system, new routine uses, and new record retention periods.

DHS Standards to Prevent, Detect, and Respond to Sexual Abuse and Assault in Confinement Facilities

Consistent with the Prison Rape Elimination Act of 2003 (PREA) (42 U.S.C. §15601 et seq.) and the Violence Against Women Reauthorization Act of 2013 (Pub. L. 113-4), DHS issued a final rule titled DHS Standards to Prevent, Detect, and Respond to Sexual Abuse and Assault in Confinement Facilities, (hereinafter, DHS PREA rule). The DHS PREA rule establishes standards to prevent, detect, and respond to sexual abuse and assault in DHS confinement facilities. The rule includes separate sets of standards tailored to two different types of confinement facilities used by DHS: (1) Immigration detention facilities, which Immigration and Customs Enforcement (ICE) oversees and uses for longer-term detention of individuals subject to immigration removal processes; and (2) holding facilities, which ICE and U.S. Customs and Border Protection (CBP) use

for temporary detention of individuals pending release from custody or transfer to a court, jail, prison, another agency, or another unit of the facility or agency.

The DHS PREA rule addresses mechanisms for individuals in DHS immigration detention or holding facilities to report to DHS incidents of sexual assault and abuse committed by DHS staff or other individuals in facilities. It also standardizes the collection and maintenance of information about known or alleged incidents of sexual assault and abuse. For additional information on the DHS PREA rule, see 6 CFR Part 115. The DHS/ALL-020 Internal Affairs SORN is being updated to provide coverage for records that will be generated by DHS in fulfilling its responsibilities under this new regulation.

Joint Integrity Case Management System

The Joint Integrity Case Management System (JICMS) is a customized application that CBP Office of Internal Affairs (IA), CBP Labor and Employee Relations (LER), ICE Office of Professional Responsibility (OPR), and ICE Employee and Labor Relations (ELR) use. ICE and CBP developed it for joint use to record misconduct, to conduct criminal and administrative investigations, and to track disciplinary actions. JICMS allows for a streamlined, integrated allegation and discipline tracking system for designated users. JICMS records continue to be included in this system of records and are covered by the DHS/ALL-020 Internal Affairs SORN.

ICE OPR Inspections

ICE's OPR inspects and reviews ICE offices, operations, and processes to provide ICE executive management with an independent review of the agency's organizational health, as well as an assessment of how effectively and efficiently ICE

carries out its mission. This includes evaluating detention facilities' compliance with ICE's detention standards. OPR conducts investigations of events in detention facilities, such as detainee deaths, allegations involving violations of civil rights and civil liberties, or non-compliance with detention standards. Records of these functions are currently covered by the DHS/ALL-020 Internal Affairs SORN to the extent information is retrieved by name or personal identifier, but the category of records has been revised to make this more explicit.

Changes to the Purpose Statement, Categories of Records, and Categories of Individuals

As described above, DHS is updating this SORN to address new records created by implementation of the DHS PREA rule and records created by ICE OPR and CBP IA when executing their oversight responsibilities. The purpose statement of this SORN also adds ICE OPR inspections and reviews (described above) to the types of internal affairs matters covered and accordingly is now broader to cover a range of internal affairs matters, such as internal compliance with laws, regulations, and policies about the overall purpose of internal affairs functions within DHS.

There are other changes in the category of records to provide clarity and completeness, such as specifically listing Alien Registration Numbers as a record category and revising the description of "investigative reports" to the more specific "investigative records of a criminal, civil, or administrative nature."

DHS is modifying the category of individuals section to provide a more comprehensive list of the types of individuals who may be subject to or involved in internal affairs matters. These include individuals held by DHS in confinement or detention facilities as well as individuals encountered, arrested, or detained by DHS or

held in DHS custody pending removal or removal proceedings under the Immigration and Nationality Act (INA) (Pub. L. 82-414). The system also includes the personally identifiable information (PII) of individuals who make allegations of sexual assault and abuse in DHS confinement facilities and individuals whose PII is provided in such allegations or over the course of any resulting investigation, including witnesses to the alleged incident or alleged abusers.

Changes to Routine Uses

DHS is revising the routine uses to improve clarity, and adding several new routine uses, including routine use U, which authorizes DHS to notify a victim following an investigation into an allegation of sexual abuse or assault of the result of the investigation, in accordance with the DHS PREA rule. Below is a general summary of all new routine uses and their corresponding letters. The actual routine uses appear in the notice.

K. To an authorized appeal or grievance examiner, formal complaints examiner, equal employment opportunity investigator, arbitrator, or other duly authorized official engaged in investigation or settlement of a grievance, complaint, or appeal filed against DHS, its employees, contractors, offices, or Components.

O. To federal, state, local, tribal, territorial, foreign, or international agencies concerning the hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, or other benefit when failure to disclose the information is likely to create a risk to public safety or to other specified interests;

P. To the Office of Personnel Management (OPM) to refer an individual who has applied for federal employment when there is falsification, deception, or fraud in the

application process; or when suitability evaluation indicates a government-wide debarment should be imposed pursuant to 5 CFR Part 731;

Q. To a former employee of DHS for purposes of responding to an official inquiry or facilitating communications with a former employee that may be relevant for personnel-related or other official purposes;

R. To federal, state, local, tribal, territorial, international, or foreign government agencies to assist in making a determination regarding a complaint or other form of redress; to verify the identity of an individual seeking redress; or to verify the accuracy of information submitted by an individual on behalf of another individual;

S. To third parties, but only that information relevant and necessary, to effectuate or to carry out a particular redress result by that third party; and

T. To notify a victim, pursuant to 6 CFR Section 115.73, following an investigation into an allegation of sexual abuse or assault, of the result of the investigation and of any responsive actions taken.

U. To notify or provide a victim or complainant of the progress or results of an investigation relating to an integrity, disciplinary inquiry, review, or inspection complaint relating to an integrity, disciplinary inquiry, review, or inspection complaint.

V. To federal, state, local, tribal, territorial, foreign, international agencies or transportation operators, when relevant or necessary to: (1) Ensure safety and security; (2) enforce safety and security-related regulations and requirements to assess and distribute intelligence or law enforcement information related to security; (3) assess and respond to threats; (4) oversee the implementation and ensure the adequacy of security measures at facilities; (5) plan and coordinate any actions or activities that may affect

safety, security, or the operations of facilities; or (6) issue, maintain, or review a license, certificate, contract, grant, or other benefit.

Information stored in the DHS/ALL-020 Internal Affairs system of records may be shared with DHS components that have a need to know the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions. In addition, consistent with DHS's information sharing mission, information may be shared with appropriate federal, state, local, tribal, territorial, foreign, or international government agencies consistent with the routine uses set forth in this system of records notice.

Changes to Record Retention

Changes to the retention period for the Department's internal affairs record systems are pending review and approval. DHS proposes that investigative, inspection, and allegation-related files be maintained for five years after the related case is closed. Records would then be transferred to the Federal Records Center (FRC) and destroyed 25 years after the date of closure for investigative files and 10 years after the date of closure for inspection and allegation-related files. Review files would be maintained for 10 years after the related case is closed, and then be transferred to the FRC and retained permanently. Sexual abuse and assault files and reports would be maintained in a secure location for 10 years after the end of the fiscal year in which the related case closed. Records then would be transferred to the FRC and destroyed 20 years after the end of the fiscal year in which the case closed.

During the course of adjudicating a complaint, records or information from other systems of records may become part of, merged with, or recompiled within this system.

This system may contain records or information compiled from or based on information contained in other systems of records that are exempt from certain provisions of the Privacy Act. To the extent this occurs, DHS will claim the same exemptions as were claimed for the original systems from which the recompiled records, material, or information were obtained. Such exempt records or information are likely to include law enforcement or investigation records, law enforcement encounter records, or possibly intelligence-related information or terrorist screening records. These could come from various DHS systems, such as TECS (DHS/CBP-011 – U.S. Customs and Border Protection TECS, 73 FR 77778 (Dec. 19, 2008)) or from other agency systems. Such records adhere to the protections described in the underlying system and are safeguarded accordingly. The originating agency consults with OPR prior to further disclosure of any such information.

II. Privacy Act

The Privacy Act embodies fair information principles in a statutory framework governing the means by which the United States Government collects, maintains, uses, and disseminates individuals' records. The Privacy Act applies to information that is maintained in a "system of records." A "system of records" is a group of any records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass United States citizens and legal permanent residents. As a matter of policy, DHS extends administrative Privacy Act protections to all individuals when systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors.

Individuals may request access to their own records that are maintained in a system of records in the possession or under the control of DHS by complying with DHS Privacy Act regulations, 6 CFR Part 5.

The Privacy Act requires each agency to publish in the Federal Register a description denoting the type and character of each system of records that the agency maintains, and the routine uses contained in each system in order to make agency record keeping practices transparent, to notify individuals regarding the uses of their records, and to assist individuals to more easily find such files within the agency. Below is the description of the DHS Internal Affairs System of Records.

In accordance with 5 U.S.C. 552a(r), DHS has provided a report of this new system of records to the Office of Management and Budget (OMB) and to Congress.

System of Records

DHS/ALL-020

System name:

DHS/ALL-020 Department of Homeland Security Internal Affairs

Security classification:

Unclassified.

System location:

Records are maintained at several Headquarters locations and in component offices of the Department of Homeland Security (DHS), in both Washington, D.C., and field locations.

Categories of individuals covered by the system:

Any individual who is subject to or involved in an internal integrity or

disciplinary inquiry, or an internal review, inspection, or investigation not handled by the DHS Office of the Inspector General (OIG). These individuals may be current or former DHS employees and contractors; contractor applicants; individuals serving in an advisory role; individuals held by DHS in confinement or detention facilities; individuals encountered, arrested, or detained by DHS or held in DHS custody pending removal or removal proceedings under the Immigration and Nationality Act (INA); individuals whose information is relevant to the investigation of alleged misconduct, including complainants, witnesses, or alleged perpetrators of sexual abuse or assault; or any other persons subject to or involved with the internal inquiries, reviews, inspections, or investigations described above.

Categories of records in the system:

Categories of records in this system include:

- Individual identifying data, which may include some or all of the following: full name, date of birth, Social Security number, Alien Registration number, addresses, contact information, duty station, grade, job series, and entrance on duty date;
- Allegations received and method received;
- Relevant information from background investigations;
- Relevant information from inspections, reviews, and inquiries, including records collected in response to an allegation of sexual abuse and assault;
- Integrity investigations records;
- Investigative records of a criminal, civil, or administrative nature;
- Incident location;

- Case agent/officer or supervisor;
- Case/prosecution status;
- Photographic images, videotapes, voiceprints, DVDs;
- Letters, e-mails, memoranda and reports;
- Exhibits, evidence, statements, and affidavits; and
- Any other information gathered in the course of or relating to an integrity or disciplinary inquiry, review, inspection, or investigation of a criminal, civil, or administrative nature, including reports generated on incidents of sexual abuse and assault.

Authority for maintenance of the system:

5 U.S.C § 301; the Federal Records Act, 44 U.S.C. § 3101; Executive Order 9397, as amended by Executive Order 13478.

Purpose(s):

The purpose of this system is to collect and maintain records concerning internal affairs matters, specifically internal integrity or disciplinary inquiries, as well as internal reviews, inspections, or investigations conducted by DHS Headquarters or its components, except those conducted by OIG. This SORN is intended to support and protect the integrity of Departmental operations; to ensure compliance with applicable laws, regulations, and policies; and to ensure the integrity of DHS employees' conduct and those acting on behalf of DHS.

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

In addition to those disclosures generally permitted under 5 U.S.C. § 552a(b) of

the Privacy Act, all or a portion of the records of information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To the Department of Justice (DOJ) (including Office of the United States Attorneys) or other federal agency conducting litigation, or in proceedings before any court, adjudicative, or administrative body when it is necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

1. DHS or any component thereof;

2. Any employee of DHS in his/her official capacity;

3. Any employee of DHS in his/her individual capacity when DOJ or DHS has agreed to represent the employee; or

4. The United States Government or any agency thereof.

B. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

C. To the National Archives and Records Administration (NARA), the General Services Administration (GSA), or any other federal agencies pursuant to records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906.

D. To an agency, organization, or individual for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

E. To appropriate agencies, entities, and persons when:

1. DHS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised;

2. DHS has determined that as a result of the suspected or confirmed compromise, there is a risk of identity theft or fraud, harm to economic or property interests, harm to an individual, or harm to the security or integrity of this system or other systems or programs (whether maintained by DHS or another agency or entity) that rely upon the compromised information; and

3. The disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

F. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

G. To an appropriate federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations, and such disclosure is proper and consistent with the official duties of the person making the disclosure.

H. To federal, state, local, tribal, territorial, foreign, or international agencies if the information is relevant and necessary to a requesting agency's decision concerning the hiring or retention of an individual, or the issuance, grant, renewal, suspension, or revocation of a security clearance, license, contract, grant, or other benefit; or if the information is relevant and necessary to a DHS decision concerning the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit.

I. To a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations in response to a subpoena from a court of competent jurisdiction.

J. To third parties during the course of a law enforcement investigation to the extent necessary to obtain information pertinent to the investigation, provided disclosure is appropriate to the proper performance of the official duties of the officer making the disclosure.

K. To an authorized appeal or grievance examiner, formal complaints examiner, equal employment opportunity investigator, arbitrator, or other duly authorized official engaged in investigation or settlement of a grievance, complaint, or appeal filed against DHS, its employees, contractors, offices, or components.

L. To provide information to unions recognized as exclusive bargaining representatives under the Civil Service Reform Act of 1978, 5 U.S.C. 7111 and 7114,

and in circumstances when union officials represent employees in investigations and personnel actions.

M. To a court, prosecutor, and/or defense attorney in satisfaction of the agency's obligations under the Jencks Act (18 U.S. 3500); *Giglio* v. *United States, 405 U.S. 150 (1972); or Brady* v. Maryland, 373 U.S. 83 (1963) decisions.

N. To management officials at federal, state, local, tribal, territorial, foreign, or international agencies who may be in a position to take disciplinary or other corrective action, and to boards and panels who may be charged with making recommendations or proposals regarding remedial action.

O. To federal, state, local, tribal, territorial, foreign, or international agencies if DHS determines: (1) The information is relevant and necessary to that agency's decision concerning the hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, or other benefit, and (2) failure to disclose the information is likely to create a risk to government facilities, equipment, or personnel; sensitive information; critical infrastructure; or the public safety.

P. To the Office of Personnel Management (OPM) to refer an individual who has applied for federal employment in cases when there is material, intentional falsification, deception, or fraud in the initial application or examination process; or when suitability evaluation indicates a government-wide debarment should be imposed pursuant to 5 CFR Part 731.

Q. To a former employee of DHS for purposes of responding to an official inquiry by federal, state, local, tribal, or territorial government agencies or professional licensing authorities; or facilitating communications with a former employee that may be

relevant and necessary for personnel-related or other official purposes when DHS requires information or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

R. To federal, state, local, tribal, territorial, foreign or international government agencies, or entities for the purpose of consulting with that agency or entity: (1) To assist in making a determination regarding a complaint or other form of redress for an individual in connection with the operations of DHS employees, contractors, components, or programs; (2) to verify the identity of an individual seeking redress in connection with the operations of a DHS component or program; or (3) to verify the accuracy of information submitted by an individual who has requested such redress on behalf of another individual.

S. To third parties lawfully authorized in connection with a federal government program, which is authorized by law, regulation, or rule, but only the information necessary and relevant to effectuate or to carry out a particular redress result for an individual and disclosure is appropriate to enable these third parties to carry out their responsibilities related to the federal government program.

T. To notify a victim, pursuant to 6 CFR Section 115.73, following an investigation into an allegation of sexual abuse or assault, of the result of the investigation and of any responsive actions taken.

U. To notify or provide a victim or complainant of information gathered on the progress or results of an investigation relating to an integrity, disciplinary inquiry, review, or inspection complaint.

V. To federal, state, local, tribal, territorial, foreign, international agencies, or transportation operators, when relevant or necessary to: (1) Ensure safety and security; (2) enforce safety and security-related regulations and requirements to assess and distribute intelligence or law enforcement information related to security; (3) assess and respond to threats; (4) oversee the implementation and ensure the adequacy of security measures at facilities; (5) plan and coordinate any actions or activities that may affect safety, security, or the operations of facilities; or(6) issue, maintain, or review a license, certificate, contract, grant, or other benefit.

W. To a federal agency or entity that furnished a record or information for the purpose of permitting that agency or entity to make a decision regarding access to or correction of the record or information.

X. To a federal agency or entity that has information relevant to an allegation or investigation for purposes of obtaining guidance, additional information, or advice from such federal agency or entity regarding the handling of this investigation, or to a federal agency or entity that was consulted during the processing of the allegation or investigation but that did not ultimately have relevant information.

Y. To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information or when disclosure is necessary to preserve confidence in the integrity of DHS or is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Disclosure to consumer reporting agencies:

None.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door. The records may be stored on magnetic disc, tape, digital media, and CD-ROM.

Retrievability:

Records may be retrieved by the individual's name, date of birth, Alien Registration Number, Social Security number, or other unique identifier.

Safeguards:

DHS safeguards records in this system in accordance with applicable rules and policies, including all applicable DHS automated systems security and access policies. DHS imposes strict controls to minimize the risk of compromising the information that is being stored. DHS limits access to the records in this system to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

Retention and disposal:

DHS is drafting a proposed records retention schedule for its internal affairs records. DHS proposes that investigative, inspection, and allegation-related files be maintained for five years after the related case is closed. Records would then be transferred to the Federal Records Center (FRC) and destroyed 25 years after the date of

closure for investigative files and ten years after the date of closure for inspection and allegation-related files. Review files will be maintained for ten years after the related case is closed. Records would then be transferred to the FRC and retained permanently. Sexual abuse and assault files and reports would be maintained in a secure location for ten years after the end of the fiscal year in which the related case is closed. Records then would be transferred to the FRC and destroyed 20 years after the end of the fiscal year in which the case was closed.

System Manager and address:

For Headquarters, the System Manager is the Chief Security Officer, Department of Homeland Security, Washington, D.C. 20528. For Components of DHS, the Chief Security Officer or component equivalent can be found at http://www.dhs.gov/department-components.

Notification procedure:

Individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the Headquarters or Component's FOIA Officer, whose contact information can be found at http://www.dhs.gov/foia under "Contacts." If an individual believes more than one component maintains Privacy Act records concerning him or her the individual may submit the request to the Chief Privacy Officer and Chief Freedom of Information Act Officer, Department of Homeland Security, 245 Murray Lane, S.W., Building 410, Mail Stop 0655, Washington, D.C. 20528.

When seeking records about yourself from this system of records or any other Departmental system of records your request must conform with the Privacy Act

regulations set forth in 6 CFR Part 5. You must first verify your identity, meaning that you must provide your full name, current address, and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. § 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Chief Privacy Officer and Chief Freedom of Information Act Officer, http://www.dhs.gov/foia or 1-866-431-0486. In addition you should provide the following:

- Explain why you believe the Department would have information on you;
- Identify which Component(s) of the Department you believe may have the information about you;
- Specify when you believe the records would have been created;
- Provide any other information that will help the FOIA staff determine which DHS Component Agency may have responsive records; and
- If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

Without this bulleted information the Component(s) may not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

Record access procedures:

See "Notification procedure" above.

Contesting record procedures:

See "Notification procedure" above.

Record source categories:

Records are obtained from individuals who are the subject of the investigation or inquiry, employers, law enforcement organizations, detention facilities, members of the public, witnesses, educational institutions, government agencies, nongovernmental organizations, credit bureaus, references, neighborhood checks, confidential sources, medical service providers, personal interviews, photographic images, military, financial institutions, citizenship, and the personnel history and application forms of agency applicants, employees or contractors.

Exemptions claimed for the system:

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).

During the course of adjudicating a complaint, records or information from other systems of records may become part of, merged with, or recompiled within this system. This system may contain records or information compiled from or based on information contained in other systems of records that are exempt from certain provisions of the Privacy Act. To the extent this occurs, DHS will claim the same exemptions as were

claimed in the original systems from which the recompiled records, material, or information were obtained.

Dated: April 2, 2014.

Karen L. Neuman,

Chief Privacy Officer,

Department of Homeland Security.

[FR Doc. 2014-09471 Filed 04/25/2014 at 8:45 am; Publication Date: 04/28/2014]