9110-9B

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS-2019-0033]

Privacy Act of 1974; System of Records

AGENCY: Privacy Office, Department of Homeland Security.

ACTION: Notice of Modified Privacy Act System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security (DHS) proposes to modify and reissue a current DHS system of records titled, "Department of Homeland Security/ALL-038 Insider Threat Program System of Records." This system of records allows DHS to establish capabilities to detect, deter, and mitigate insider threats. An "Insider" is defined to include any person who has or who had authorized access to any DHS facility, information, equipment, network, or system. An "insider threat" is the threat that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the Department's mission, resources, personnel, facilities, information, equipment, networks, or systems. DHS will use the system to facilitate management of insider threat inquiries; identify potential threats to DHS resources and information assets; manage referrals of potential insider threats to and from internal and external partners; provide authorized assistance to lawful administrative, civil, counterintelligence, and criminal investigations; and provide statistical reports and meet other insider threat reporting requirements.

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

effective **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: You may submit comments, identified by docket number DHS-2019-0033 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: Jonathan R. Cantor, Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528-0655.

Instructions: All submissions received must include the agency name and docket number DHS-2019-0033. All comments received will be posted without change to http://www.regulations.gov, including any personal information provided.

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

FOR FURTHER INFORMATION CONTACT: For general questions, please contact: Jonathan R. Cantor, (202) 343-1717, Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528-0655.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. sec. 552a, Department of Homeland Security (DHS) proposes to modify and reissue a current DHS system of records titled, "DHS/ALL-038 Insider Threat Program System of Records."

DHS developed an Insider Threat Program (ITP) to manage insider threat matters within DHS. The ITP is mandated by Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," issued October 7, 2011, which requires Federal agencies to establish an insider threat detection and prevention program to ensure the security of classified networks and the responsible sharing and safeguarding of classified information with appropriate protections for privacy and civil liberties.

DHS is modifying the Insider Threat Program System of Records to account for the new population affected and new types of information the program is now authorized to collect and maintain pursuant to a memorandum, *Expanding the Scope of the Department of Homeland Security Insider Threat Program*, submitted to the Secretary of Homeland Security on December 7, 2016, and approved on January 3, 2017. Originally, the Insider Threat Program focused on the detection, prevention, and mitigation of unauthorized disclosure of classified information by DHS personnel with active security clearances. The Secretary's memorandum expands the scope of the Insider Threat Program to its current breadth: threats posed to the Department by *all* individuals who have or had access to the Department's facilities, information, equipment, networks, or systems. Unauthorized disclosure of classified information is merely one way in which this threat might manifest. Therefore, the expanded scope increases the population covered by the system to include all those with past or current access to DHS facilities, information, equipment, networks, or systems.

Therefore, the Department is modifying the category of individuals covered under this SORN to all individuals who have or had access to the Department's facilities, information, equipment, networks, or systems.

The category of records in this SORN will be modified to cover records from any DHS Component, office, program, record, or source, including records from information security, personnel security, and systems security for both internal and external security threats. Information contained in such records is necessary to identify, analyze, or resolve insider threat matters. Moreover, the Insider Threat Program system of records may include information lawfully obtained from any United States Government Agency, DHS Component, other domestic or foreign government entity, and from a private sector entity. DHS is also updating Routine Use E and adding Routine Use F to comply with requirements set forth by OMB Memorandum M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information," (Jan. 3, 2017). Additionally, this notice includes non-substantive changes to simplify the formatting and text of the previously published notice.

Consistent with DHS's information sharing mission, information stored in the DHS/ALL-038 Insider Threat Program system of records may be shared with other 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, DHS may share information with appropriate federal, state, local, tribal, territorial, foreign, or international government agencies and private sector partners consistent with the routine uses set forth in this system of records notice.

Furthermore, DHS is issuing a Notice of Proposed Rulemaking to exempt this

system of records from certain provisions of the Privacy Act elsewhere in the Federal Register. This modified system will be included in DHS's inventory of record systems.

II. Privacy Act

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which Federal Government agencies collect, maintain, use, and disseminate 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 U.S. citizens and lawful permanent residents. Additionally, the Judicial Redress Act (JRA) provides covered persons with a statutory right to make requests for access and amendment to covered records, as defined by the JRA, along with judicial review for denials of such requests. In addition, the JRA prohibits disclosures of covered records, except as otherwise permitted by the Privacy Act.

Below is the description of the DHS/ALL-038 Insider Threat Program System of Records. In accordance with 5 U.S.C. sec. 552a(r), DHS has provided a report of this system of records to the Office of Management and Budget and to Congress.

SYSTEM NAME AND NUMBER: Department of Homeland Security (DHS) DHS/ALL-038 Insider Threat Program System of Records.

SECURITY CLASSIFICATION: Unclassified and Classified.

SYSTEM LOCATION: Records are maintained at several DHS Headquarters and Component locations in Washington, D.C. and field offices.

SYSTEM MANAGER(S): Program Manager, Insider Threat Operations Center (202-447-5010), Office of the Chief Security Officer, Department of Homeland Security, Washington, D.C. 20528.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Intelligence Reform and Terrorism Prevention Act of 2004, Public Law 108-458; Intelligence Authorization Act for FY 2010, Public Law 111-259; Atomic Energy Act of 1954, 60 Stat. 755, August 1, 1946; Under Secretary for Management, Title 6 U.S.C. 341(a)(6); Investigation of Crimes Involving Government Officers and Employees, Title 28 U.S.C. 535; Law Enforcement Authority of Secretary of Homeland Security for Protection of Public Property, Title 40 U.S.C. 1315; Coordination of Counterintelligence Activities, Title 50 U.S.C. 3381; Executive Order 10450, Security Requirements for Government Employment, 18 Fed. Reg. 2,489 (April 17, 1953); Executive Order 12333, United States Intelligence Activities, 46 Fed. Reg. 59,941 (December 4, 1981), *reprinted as amended* in 73 Fed. Reg. 45,325 (July 30, 2008); Executive Order 12829, National Industrial Security Program, 58 Fed. Reg. 3,479 (January 06, 1993), *reprinted as amended in part* in 80 Fed. Reg. 60,271 (September 30, 2015); Executive Order 12968, Access to Classified Information, 60 Fed. Reg. 40,245 (August 2, 1995); Executive Order 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information, 73 Fed. Reg. 38,103 (June 30, 2008), *reprinted as amended in part* in 82 Fed. Reg. 8115 (January 17, 2017); Executive Order 13488, Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust, 74 Fed. Reg. 4,111 (January 16, 2009), *reprinted as amended in part* in 82

FR 8115 (January 17, 2017); Executive Order 13526, Classified National Security Information, 75 Fed. Reg. 707 (December 29, 2009); Executive Order 13549, Classified National Security Information Programs for State, Local, Tribal, and Private Sector Entities, 75 Fed. Reg. 51,609 (August 18, 2010), *reprinted as amended* in 80 Fed. Reg. 60,271 (September 30, 2015); Executive Order 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, 76 Fed. Reg. 63,811 (October 7, 2011); and Presidential Memorandum National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs (November 21, 2012).

PURPOSE(S) OF THE SYSTEM: The purpose of this system is to detect, deter, and mitigate insider threats. DHS will use the system to facilitate management of insider threat inquiries; identify and track potential insider threats to DHS; manage referrals of potential insider threats to and from internal and external partners; provide authorized assistance to lawful administrative, civil, counterintelligence, and criminal investigations; and generate statistical reports and meet other insider threat reporting requirements.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: The categories of individuals covered by this system are DHS "insiders," as defined above, which include present and former DHS employees, contractors, detailees, assignees, interns, visitors, and guests. In addition, persons who report concerns, witnesses, relatives, and individuals with other relevant personal associations with a DHS insider are covered by the system of records notice.

CATEGORIES OF RECORDS IN THE SYSTEM: The system may collect the following types of information:

- Information potentially relevant to resolving possible insider threats and lawful DHS security investigations, including authorized physical, personnel, and communications security investigations, and information systems security analysis and reporting. Such information may include:
    - Individual's name and alias(es);
    - Date and place of birth;
    - Social Security number;
    - Address;
    - Open source information, including publicly available social media information;
    - Personal and official email addresses;
    - Citizenship;
    - Personal and official phone numbers;
    - Driver license number(s);
    - Vehicle Identification Number(s);
    - License plate number(s);
    - Ethnicity and race;
    - Current Employment and Performance Information;

- Work history;
- Education history;
- Contract information;
- Information on family members, dependents, relatives and other personal associations;
- Passport number(s);
- DHS-held Travel records;
- Gender;
- Hair and eye color;
- Biometric data;
- Other physical or distinguishing attributes of an individual;
- Medical information;
- Access control pass, credential number, or other identifying number(s);
- Media obtained through authorized procedures, such as CCTV footage; and
- Any other information provided to obtain access to DHS facilities or information systems.

- Records relating to the management and operation of the DHS physical, personnel, and communications security programs, including:
    - Completed standard form questionnaires issued by the Office of Personnel Management;
    - Background investigative reports and supporting documentation, including criminal background, medical, and financial data;
    - Current and former clearance status(s);
    - Other information related to an individual's eligibility for access to classified information;
    - Criminal history records;
    - Polygraph examination results;
    - Logs of computer activities on all DHS IT systems or any IT systems accessed by DHS personnel;
    - Nondisclosure agreements;
    - Document control registries;
    - Courier authorization requests;
    - Derivative classification unique identifiers;
    - Requests for access to sensitive compartmented information (SCI);
    - Records reflecting personal and official foreign travel;

- Facility access records;
- Records of contacts with foreign persons; and
- Briefing/debriefing statements for special programs, sensitive positions, and other related information and documents required in connection with personnel security clearance determinations.

- Reports of investigations or inquiries regarding security violations or misconduct, including:
  - Individuals' statements or affidavits and correspondence;
  - Incident reports;
  - Drug test results;
  - Investigative records of a criminal, civil, or administrative nature;
  - Letters, emails, memoranda, and reports;
  - Exhibits, evidence, statements, and affidavits;
  - Inquiries relating to suspected security violations;
  - Recommended remedial actions for possible security violations; and
  - Personnel files containing information about misconduct and adverse actions.

- Any information related to the management and operation of the DHS ITP, including:

- Documentation pertaining to fact-finding or analytical efforts by ITP personnel to identify insider threats to DHS resources, personnel, property, facilities, or information;
- Records of information technology events and other information that could reveal potential insider threat activities;
- Intelligence reports and database query results relating to individuals covered by this system;
- Information obtained from the Intelligence Community, law enforcement partners, and from other agencies or organizations about individuals and/or organizations known or reasonably suspected of being engaged in conduct constituting, preparing for, aiding, or relating to an insider threat;
- Information provided by subjects and individual members of the public; and
- Information provided by individuals who report known or suspected insider threats.

RECORD SOURCE CATEGORIES: Records are obtained from (1) software that monitors DHS users' activity on U.S. Government computer networks; (2) information supplied by individuals to the Department or by the individual's employer; (3) information provided to the Department to gain access to DHS facilities, information, equipment, networks, or systems; (4) publicly available information obtained from open source platforms, including publicly available social media; (5) any departmental records

for which the ITP has been given authorized access; and (6) any federal, state, tribal, local government, or private sector records for which the ITP has been given authorized access. The Insider Threat Operations Center (ITOC) also receives tips and leads by other means, such as email or telephone. The ITOC may receive a tip from any party, including members of the public.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES: In addition to those disclosures generally permitted under 5 U.S.C. sec. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. sec. 552a(b)(3) as follows:

A. To the Department of Justice (DOJ), including the U.S. Attorneys Offices, or other federal agency conducting litigation or proceedings before any court, adjudicative, or administrative body, when it is relevant or 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 or former employee of DHS in his/her official capacity;

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

4. The United States 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) or General Services Administration pursuant to records management inspections being conducted under the authority of 44 U.S.C. sec. 2904 and 2906.

D. To an agency or organization 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 there has been a breach of the system of records; (2) DHS has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DHS (including its information systems, programs, and operations), the Federal Government, or national security; 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 breach or to prevent, minimize, or remedy such harm.

F. To another Federal agency or Federal entity, when DHS determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

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 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.

I. To an appropriate Federal, state, local, tribal, territorial, foreign, or international agency, if the information is relevant and necessary to a requesting agency's decision concerning the hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, delegation or designation of authority, 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, delegation or designation of authority, or other benefit and disclosure is appropriate to the proper performance of the official duties of the person making the request.

J. To a prospective or current employer that has, or is likely to have, access to any government facility, information, equipment, network, or system, to the extent necessary to determine the employment eligibility of an individual, based on actions taken by the Department pursuant to an insider threat inquiry involving the individual.

K. To third parties during the course of an 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 individual making the disclosure.

L. To a public or professional licensing organization when such information indicates, either by itself or in combination with other information, a violation or potential violation of professional standards, or reflects on the moral, educational, or professional qualifications of an individual who is licensed or who is seeking to become licensed.

M. To another federal agency in order to conduct or support authorized counterintelligence activities, as defined by 50 U.S.C. 3003(3).

N. To any Federal, state, local, tribal, territorial, foreign, or multinational government or agency, or appropriate private sector individuals and organizations lawfully engaged in national security or homeland defense for that entity's official responsibilities, including responsibilities to counter, deter, prevent, prepare for, respond to, threats to national or homeland security, including an act of terrorism or espionage.

O. To a Federal, state, local, tribal, or territorial government or agency lawfully engaged in the collection of intelligence (including national intelligence, foreign intelligence, and counterintelligence), counterterrorism, homeland security, law enforcement or law enforcement intelligence, and other information, when disclosure is undertaken for intelligence, counterterrorism, homeland security, or related law enforcement purposes, as authorized by U.S. Law or Executive Order.

P. To any individual, organization, or entity, as appropriate, to notify them of a serious threat to homeland security and/or a potential insider threat for the purpose of

guarding them against or responding to such a threat, or when there is a reason to believe that the recipient is or could become the target of a particular threat, to the extent the information is relevant to the protection of life, health, or property.

Q. To members of the U.S. House Committee on Oversight and Reform and the Senate Homeland Security and Governmental Affairs Committee pursuant to a written request under 5 U.S.C. 2954, after consultation with the Chief Privacy Officer and the General Counsel.

R. To a federal agency or entity that has information relevant to an allegation or investigation regarding an insider threat for purposes of obtaining guidance, additional information, or advice from such federal agency or entity regarding the handling of an insider threat matter, 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.

S. To a former DHS employee, DHS contractor, or individual sponsored by DHS for a security clearance 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.

T. 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, when disclosure is necessary to preserve confidence in the

integrity of DHS, or when disclosure is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent the Chief Privacy Officer determines that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: DHS/ALL-038 Insider Threat Program stores records in this system electronically or on paper in secure facilities in a locked drawer behind a locked door. The records may be stored on magnetic disc, tape, and digital media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: DHS may retrieve records by first and last name, Social Security number, date of birth, phone number, other unique individual identifiers, and other types of information by key word search.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: In accordance with General Records Schedule 5.6: Security Records (July 2017), Insider Threat (a) records pertaining to an "insider threat inquiry" are destroyed 25 years after the close of the inquiry; (b) records containing "insider threat information" are destroyed when 25 years old; (c) insider threat user activity monitoring (UAM) data is destroyed no sooner than 5 years after the inquiry has been opened, but longer retention is authorized if required for business use; and (d) insider threat administrative and operations records are destroyed when 7 years old.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: DHS ITP safeguards records in this system according to applicable rules and policies, including all applicable DHS automated systems security and access policies. DHS has imposed strict

controls to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited 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.

RECORD ACCESS PROCEDURES: As described below, this system of records is exempt from the notification, access, and amendment provisions of the Privacy Act, and the Judicial Redress Act if applicable. However, DHS will consider individual requests to determine whether or not information may be released. Individuals seeking access to and notification of any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the Chief Privacy Officer and Headquarters FOIA Officer, whose contact information can be found at http://www.dhs.gov/foia under "Contacts Information." 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, Washington, D.C. 20528-0655. Even if neither the Privacy Act nor the Judicial Redress Act provides a right of access, certain records about you may be available under the Freedom of Information Act.

When an individual is seeking records about himself or herself from this system of records or any other Departmental system of records, the individual's request must conform with the Privacy Act regulations set forth in 6 CFR Part 5. The individual must first verify his/her identity, meaning that the individual must provide his/her full name, current address, and date and place of birth. The individual must sign the request, and the individual's signature must either be notarized or submitted under Title 28 U.S.C. sec.

1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, an individual 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, the individual should:

- Explain why he or she believes the Department would have information being requested;
- Identify which component(s) of the Department he or she believes may have the information;
- Specify when the individual believes the records would have been created; and
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records;

If the request is seeking records pertaining to another living individual, the request must include an authorization from the individual whose record is being requested, authorizing the release to the requester.

Without the above information, the component(s) may not be able to conduct an effective search, and the individual's request may be denied due to lack of specificity or lack of compliance with applicable regulations.

CONTESTING RECORD PROCEDURES: For records covered by the Privacy Act or Judicial Redress Act-covered records, individuals may make a request for amendment or correction of a record of the Department about the individual by writing directly to the Department component that maintains the record. The request should identify each particular record in question, state the amendment or correction desired, and state why the individual believes that the record is not accurate, relevant, timely, or complete. The

individual may submit any documentation that would be helpful. If the individual believes that the same record is in more than one system of records, the request should state that and be addressed to each component that maintains a system of records containing the record.

NOTIFICATION PROCEDURES: See "Record Access Procedures" above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: 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), (e)(12); (f); and (g)(1). Additionally, 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 this system receives a record from another system exempted in that source system under Title 5 U.S.C. 552a(j)(2), 5 U.S.C. § 552a(k)(1), (k)(2), and (k)(5), 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.

HISTORY: 81 Fed. Reg. 9,871 (February 26, 2016)

Jonathan R. Cantor,

Acting Chief Privacy Officer,

Department of Homeland Security.

[FR Doc. 2020-04795 Filed: 3/9/2020 8:45 am; Publication Date: 3/10/2020]