9111-14

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2016-0067]

Privacy Act of 1974; Department of Homeland Security, United States Customs and Border Protection DHS/CBP-023 Border Patrol Enforcement Records, 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 establish a new Department of Homeland Security system of records titled, "Department of Homeland Security (DHS)/U.S. Customs and Border Protection (CBP)-023 Border Patrol Enforcement Records (BPER) System of Records." This system of records contains information DHS/CBP collects and maintains to secure the U.S. border between the Ports of Entry (POE), furthering its enforcement and immigration mission. DHS previously maintained these records under the DHS/ICE-011 U.S. Immigration and Customs Enforcement Operational Records (ENFORCE) (April 30, 2015, 80 FR 24269) and the DHS/USVISIT-004 DHS Automated Biometric Identification System (IDENT) (June 5, 2007, 72 FR 31080) System of Records Notices (SORNs), as part of a DHS-wide initiative in 2008 to restructure the former INS-012 Deportable Alien Control System (DACS) SORN.

DHS/CBP is issuing this new system of records to claim ownership of records

created as a result of CBP interactions between the POE. CBP inputs non-intelligence information it collects as a result of these interactions into its E3 Portal. CBP also collects and maintains information related to camera and sensor alerts in its Intelligent Computer Assisted Detection (ICAD) database. This system of records applies to the categories of information input and maintained in these systems. This information includes biographic, biometric, geolocation imagery and coordinates, and other enforcement and detention data associated with encounters, investigations, border violence, seized property in relation to an apprehension, inspections, prosecutions, and custody operations of DHS/CBP between the ports of entry for law enforcement, immigration, or border security purposes.

Additionally, the Department of Homeland Security 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 newly established system of records will be included in the Department of Homeland Security's inventory of record systems.

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 DATE OF PUBLICATION IN THE FEDERAL REGISTER**].

ADDRESSES: You may submit comments, identified by docket number DHS-2016-0067 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.

INSTRUCTIONS: All submissions received must include the agency name and docket number for this rulemaking. 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, please visit http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: For general questions, please contact: Debra L. Danisek, (202) 344-1610, Acting Privacy Officer, U.S. Customs and Border Protection, Washington, D.C. 20229. For privacy questions, please contact: Jonathan R. Cantor, (202) 343-1717, Acting 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. sec. 552a, the Department of Homeland Security (DHS)/U.S. Customs and Border Protection (CBP) proposes to establish a new DHS system of records titled, "DHS/CBP-023 Border Patrol Enforcement Records (BPER) System of Records."

This system of records contains information DHS/CBP collects and maintains to prevent the illegal entry of people, terrorists, terrorist weapons, and contraband from entering the United States between the Ports of Entry (POE) (for records collected at the

POE, either for lawful admission or entry to the United States or for enforcement purposes, please see DHS/CBP-007 Border Crossing Information (BCI) (January 25, 2016, 81 FR 4040 and DHS/CBP-011 U.S. Customs and Border Protection TECS (December 19, 2008 73 FR 77778), respectfully). DHS previously covered these records under the DHS/ICE-011 U.S. Immigration and Customs Enforcement (ICE) Operational Records (ENFORCE) (April 30, 2015, 80 FR 24269) and the DHS/NPPD-004 DHS Automated Biometric Identification System (IDENT) (June 5, 2007, 72 FR 31080) SORNs, as part of a DHS-wide initiative in 2008 to restructure the former Immigration and Naturalization Service (INS)-012 DACS SORN.

DHS/CBP is issuing this new system of records to claim ownership of records created as a result of CBP interactions between the POE. CBP inputs non-intelligence information it collects as a result of these interactions into its E3 Portal,[1] which serves as a conduit to ICE Enforcement and Integrated Database (EID) and DHS Office of Biometric Identity Management (OBIM) IDENT (for biometric storage). CBP also collects and maintains information related to camera and sensor alerts in its ICAD database.[2] This system of records applies to the categories of information input and maintained in these systems. This information includes biographic, biometric, geolocation imagery and coordinates, and other enforcement and detention data associated with encounters, investigations, border violence, seized property in relation to an apprehension, inspections, prosecutions, and custody operations of DHS/CBP between

[1] DHS/CBP/PIA-012 CBP Portal (E3) to ENFORCE/IDENT (July 25, 2012), available at https://www.dhs.gov/publication/cbp-portal-e3-enforceident.
[2] DHS/CBP/PIA-022 Border Surveillance Systems (BSS) (August 29, 2014), available at https://www.dhs.gov/publication/border-surveillance-systems-bss.

the ports of entry for law enforcement, immigration, or border security purposes.

CBP, through the U.S. Border Patrol (USBP), plays a critical role in securing the U.S. borders between POE against all threats. CBP/USBP prevent terrorists and terrorist weapons from entering the United States between the POE through improved and focused intelligence-driven operations and enhanced integration, planning, and execution of operations with law enforcement partners. CBP/USBP manages risk through the introduction and expansion of sophisticated technologies, tactics, techniques, and procedures, including mobile-response capabilities. CBP/USBP enforces the law, primarily immigration and customs laws, performs related homeland security functions, and disrupts and degrades Transnational Criminal Organizations (TCO) by targeting enforcement efforts against the highest priority threats and expanding programs that reduce smuggling and crimes associated with smuggling.

To facilitate and further the overall CBP/USBP goal to secure the U.S. borders, DHS/CBP uses BPER to collect, store, and retrieve geolocation imagery and coordinates, biographic, and biometric records about individuals, vehicles, vessels, property, or aircrafts encountered, apprehended, or seized between POE. These records include encounters of individuals (including U.S. citizens and non-U.S. citizens) between POE, related to border crossing events and activities, and information associated with individuals that are detected, apprehended, detained, or involved with surveillance technologies. These encounters can also include information about Border Patrol Agents and assaults made against them, as well as the use of force that may be necessarily exercised during an encounter.

BPER can include any associated encounter, enforcement, or detection information (including citizen reports) to assist CBP in making determinations about individuals that violated, or are suspected of violating, a law or regulation that is enforced or administered by DHS/CBP. DHS/CBP may use BPER information to determine immigration or citizenship status, eligibility for immigration benefits, to prosecute individuals apprehended for violation of U.S. laws enforced by DHS, and for other uses related to the enforcement of U.S. laws. DHS/CBP will also use BPER records to carry out its national security, law enforcement, immigration, and other homeland security functions.

Consistent with DHS's information sharing mission, information stored in DHS/CBP-023 BPER may be shared with other DHS components that have a need to know the information in order to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions. In addition, DHS/CBP may share information 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.

Additionally, 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 newly established 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. 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.

Below is the description of the DHS/CBP-023 Border Patrol Enforcement Records, 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 of Records

Department of Homeland Security (DHS)/U.S. Customs and Border Protection-023

System name:

DHS/CBP-023 Border Patrol Enforcement Records (BPER)

Security classification:

Unclassified. The data may be retained on the classified networks but this does not change the nature and character of the data until it is combined with classified information.

System location:

DHS/CBP primarily maintains records at the CBP Headquarters offices in Washington, D.C. and at Office of Border Patrol Sector and Station locations. BPER are primarily collected and or maintained within three information technology systems (E3 Portal, U.S. Immigration and Customs Enforcement (ICE) EID, and the ICAD database), however these records may also be stored locally by Sector or Station offices, checkpoints, mobile information collection devices, and border surveillance technologies. This system of record notice encompasses the categories of information currently input and or maintained in E3, EID, and ICAD. On behalf of CBP, DHS stores BPER biometric records in the DHS biometrics repository, OBIM IDENT.[3]

DHS/CBP also replicates records from these operational systems and maintains them on other DHS unclassified and classified systems and networks.

Categories of individuals covered by the system:

Categories of individuals covered by this system of records include:

1. Individuals encountered, apprehended, detained, or removed in relation to border crossings, checkpoint operations, law enforcement actions and investigations, inspections, patrols, examinations, legal proceedings, or other operations that implement and enforce the Immigration and Nationality Act (INA) (8 U.S.C. 1101 et seq.) and related treaties, statutes, orders, and regulations;

[3] DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT), and Appendices (December 7, 2012), available at https://www.dhs.gov/publication/dhsnppdpia-002-automated-biometric-identification-system.

2. Individuals wanted by other law enforcement agencies, including federal, state, local, tribal, foreign, and international, or individuals who are the subject of inquiries, lookouts, or notices by another agency or a foreign government; and
3. Individuals who contact DHS/CBP with complaints, tips, leads, or other information regarding a violation, or potential violation, of laws enforced by DHS/CBP.

Categories of records in the system:

Categories of records in this system include:

1. Biographic, descriptive, historical, and other identifying data, including but not limited to: names; aliases; fingerprint identification number (FIN) or other biometric identifying numbers; date and place of birth; passport and other travel or identification document information; nationality; aliases; Alien Registration Number (A-Number); Social Security number (SSN); contact or location information (e.g., known or possible addresses, phone numbers); employment, educational, immigration, and criminal history; marital status; occupation; height, weight, eye color, hair color, and other unique physical characteristics (e.g., scars and tattoos). Identifying information also includes vehicle, vessel, and aircraft identifying information, such as license plate numbers, even if not directly related to an individual at the time of collection.
2. Biometric data including: fingerprints, iris scans, blood type, and photographs. Biometric information is obtained directly from individuals, and from matches

against other Government biometric databases. Biometric data is not normally collected for individuals under the age of 14.

3. Geolocation imagery and coordinates including: sensor alerts and camera images of individuals, vehicles, vessels, or aircraft and the time, date, and location of the image.
4. Enforcement-related data including: case number, record number, and other data describing an event involving alleged violations of criminal, immigration, or other laws (location, date, time, event category, types of criminal or immigration law violations alleged, types of property involved, use of violence, weapons, or assault against DHS personnel or third parties, attempted escape, and other related information); CBP encounter management information, including: category (event categories describe broad categories of criminal law enforcement, such as smuggling and human trafficking), agent or officer, location of officer or officer's vehicle, date/time initiated, date/time completed, assets used for encounter (bike, horse, vehicle, etc.), results of the encounter, and any agent or officer notes and comments.
5. Data on aliens in custody or detained, including: transportation information, identification numbers, custodial actions (such as meals, conditions of detainee cell, overall detainee care information), custodial property, information related to detainers, book-in/book-out date and time, and other alerts.
6. Limited health information gathered during a temporary detention in a CBP facility or otherwise relevant to transportation requirements.

7. Contact, biographical, and identifying data of relatives, associates of an alien (which may include information for individuals such as an attorney), or witnesses to an encounter, but not limited to: name, date of birth, place of birth, address, telephone number, and business or agency name.
8. Alerts, typically containing biographic but occasionally biometric information, concerning individuals who are the subject of inquiries, lookouts, or notices by another federal agency, state, local, tribal, territorial, or foreign government.
9. Data concerning personnel of other agencies that arrested, or assisted or participated in the arrest or investigation of, or are maintaining custody of, an individual whose arrest record is contained in this system of records. This can include: name, title, agency name, address, telephone number, and other information.
10. Basic contact information, including name, phone numbers, and address, from members of the public who voluntarily contact DHS with complaints, tips, leads, or information about violations, or potential violations, of law.

Authority for maintenance of the system:

5 U.S.C. sec. 301; 6 U.S.C. sec. 202; 8 U.S.C. secs. 1103, 1185, 1225, 1357, 1365a, 1365b, 1379, and 1732; 19 U.S.C. secs. 482, 1461, 1496, 1581, 1582; Homeland Security Act of 2002 (Pub. L. 107-296); Justice for All Act of 2004 (Pub. L. 108-405); Intelligence Reform and Terrorism Prevention Act of 2004 (Pub. L. 108-458); Secure Fence Act of 2006 (Pub. L. 109, 367); 8 CFR 287.

Purpose(s):

The purposes of this system of records are to:

1. Prevent the entry of inadmissible aliens into the United States;
2. Record the detection, location, encounter, identification, apprehension, and/or detention of individuals who commit violations of U.S. laws enforced by CBP or DHS between the POE;
3. Support the identification and arrest of individuals (both citizens and non-citizens) who commit violations of federal criminal laws enforced by DHS;
4. Support the grant, denial, and tracking of individuals who seek or receive parole into the United States;
5. Provide criminal and immigration history information during DHS enforcement encounters, and background checks on applicants for DHS immigration benefits (e.g., employment authorization and petitions); and
6. Identify potential terrorist and criminal activity, immigration violations, and threats to homeland security; to uphold and enforce the law; and to ensure public safety.

DHS/CBP maintains a replica of some or all of the data in the operating system on other unclassified and classified systems and networks to allow for analysis and vetting consistent with the above stated purposes and this published notice.

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. 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, including Offices of the United States Attorneys, or other federal agency conducting litigation or in 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 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 pursuant to a written Privacy Act waiver 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. secs. 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 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 appropriate federal, state, tribal, local, or foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, or license, when DHS/CBP believes the information would assist in the enforcement of applicable civil or criminal laws;

I. To federal and foreign government intelligence or counterterrorism agencies or components when DHS/CBP becomes aware of an indication of a threat or potential threat to national or international security, or when such use is to assist in the anti-terrorism efforts and disclosure is appropriate in the proper performance of the official duties of the person making the disclosure;

J. To a federal, state, or local agency, or other appropriate entity or individual, or through established liaison channels to selected foreign governments, in order to provide intelligence, counterintelligence, or other information for the purposes of intelligence, counterintelligence, or antiterrorism activities authorized by U.S. law, Executive Order, or other applicable national security directive;

K. To an organization or person in either the public or private sector, either foreign or domestic, when there is a reason to believe that the recipient is or could become the target of a particular terrorist activity or conspiracy, or when the information is relevant to the protection of life, property, or other vital interests of a person;

L. 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, or in connection with criminal law proceedings;

M. 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 in the proper performance of the official duties of the officer making the disclosure;

N. To other federal agencies for the purposes of biometric identity verification and resolution, such as the Department of Defense (DoD) Automated Biometric Information System and the DOJ Next Generation Identification (NGI);

O. To foreign governments for the purpose of coordinating and conducting the removal of aliens to other nations, including issuance of relevant travel documents; and to international, foreign, and intergovernmental agencies, authorities, and organizations in accordance with law and formal or informal international arrangements;

P. To federal, state, local, territorial, tribal, and foreign law enforcement or custodial agencies for the purpose of placing an immigration detainer on an individual in that agency's custody, or to facilitate the transfer of custody of an individual from CBP to the other agency. This will include the transfer of information about unaccompanied minor children to the U.S. Department of Health and Human Services (HHS), Office of Refugee Resettlement (ORR), to facilitate the custodial transfer of such children from CBP to HHS;

Q. To appropriate federal, state, local, tribal, foreign governmental agencies, multilateral governmental organizations, or other public health entities, for the purpose of protecting the vital interests of a data subject or other persons, including to assist such agencies or organizations in preventing exposure to or transmission of a communicable or quarantinable disease or to combat other significant public health threats; appropriate notice will be provided of any identified health threat or risk;

R. To appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations when CBP is aware of a need to use relevant data for purposes of testing new technology and systems designed to enhance border security or identify other violations of law.

S. 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 the Chief Privacy Officer determines that the 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:

DHS/CBP stores records in this system electronically (on unclassified and classified systems and networks) 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, or in any other electronic form.

Retrievability:

DHS/CBP may be retrieve records by name or other personal identifiers listed in the categories of records, above.

Safeguards:

DHS/CBP safeguards records in this system according to applicable rules and policies, including all applicable DHS automated systems security and access policies. DHS/CBP has imposed strict controls to minimize the risk of compromising the information that is being stored. Access to the computer systems containing the records in this system of records is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate permissions.

Retention and disposal:

CBP is in the process of drafting a proposed record retention schedule for the information maintained in the BPER SORN. CBP anticipates retaining records of arrests, detentions, and removals for seventy-five (75) years. Investigative information that does not result in an individual's arrest, detention, or removal, is stored for twenty (20) years after the investigation is closed, consistent with the N1-563-08-4-2. User account management records for ten (10) years following an individual's separation of

employment from federal service; statistical records for ten (10) years; audit files for fifteen (15) years; and backup files for up to one (1) month. Records replicated on other DHS or CBP unclassified and classified systems and networks will follow the same retention schedule.

System Manager and address:

Associate Chief, U.S. Border Patrol, Enforcement Systems Branch, U.S. Customs and Border Protection, 1300 Pennsylvania Avenue, NW, Washington, D.C. 20229.

Notification procedure:

The Secretary of Homeland Security has exempted this system from the notification, access, accounting, and amendment procedures of the Privacy Act because it is a law enforcement system. However, DHS/CBP will consider individual requests to determine whether or not information may be released. Thus, 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 Chief Privacy Officer and Headquarters or CBP Freedom of Information Act (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 Drive, SW, Building 410, 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 5.20, et seq. 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. 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, 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:

- 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; and
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records;

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 the above 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.

In processing Privacy Act requests for related to information in this system, DHS/CBP will review the records in the operational system, and coordinate review of records that were replicated on other unclassified and classified systems and networks.

Record access procedures:

See "Notification procedure" above.

Contesting record procedures:

See "Notification procedure" above.

Record source categories:

Records in the system are supplied by several sources. In general, information is obtained from individuals covered by this system, and other federal, state, local, tribal, or foreign governments. More specifically, DHS/CBP-023 BPER derive from the following sources:

a) Individuals covered by the system and other individuals (e.g., witnesses, family members);
b) Other federal, state, local, tribal, or foreign governments and government information systems;
c) Business records;
d) Evidence, contraband, and other seized material; and
e) Public and commercial sources.

Exemptions claimed for the system:

The Secretary of Homeland Security has exempted portions of this system of records from subsecs. (c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(5),

and (e)(8); and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2). In addition, the Secretary of Homeland Security has exempted portions of this system of records from subsections (c)(3); (d); (e)(1), (e)(4)(G), and (e)(4)(H) of the Privacy Act 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(j)(2) and (k)(2). In addition, to the extent a record contains information from other exempt systems of records, DHS will rely on the exemptions claimed for those systems.

Dated: October 5, 2016

Jonathan R. Cantor,
Acting Chief Privacy Officer,
Department of Homeland Security.
[FR Doc. 2016-25206 Filed: 10/19/2016 8:45 am; Publication Date: 10/20/2016]