



DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS-2020-0017]

Privacy Act of 1974; System of Records

AGENCY: U.S. Customs and Border Protection, U.S. Department of Homeland Security.

ACTION: Notice of Modified Privacy Act System of Records.

SUMMARY: The U.S. Department of Homeland Security (DHS)/U.S. Customs and Border Protection (CBP) proposes to modify and reissue an existing system of records titled, “DHS/CBP-024 CBP Intelligence Records System (CIRS).” CIRS contains information collected by CBP to support CBP’s law enforcement intelligence mission. This information includes raw intelligence information collected by CBP’s Office of Intelligence (OI), public source information, and information initially collected by CBP pursuant to its immigration and customs authorities, which is then analyzed and incorporated into intelligence products.

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-2020-0017 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: Constantina Kozanas, Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, D.C. 20528.

Instructions: All submissions received must include the agency name and docket number DHS-2020-0017. 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: Debra L. Danisek (202) 344-1610, privacy.cbp@cbp.dhs.gov, CBP Privacy Officer, U.S. Customs and Border Protection, 1300 Pennsylvania Avenue N.W., Washington, D.C. 20229. For privacy questions, please contact: Constantina Kozanas, (202) 343-1717, Privacy@hq.dhs.gov, Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

CBP currently uses the Analytical Framework for Intelligence (AFI) and the Intelligence Reporting System (IRS) to facilitate the development of finished intelligence products. Information collected by CBP for an intelligence purpose that is not covered by an existing DHS System of Records Notice (SORN) and is not incorporated into a finished intelligence product is retained and disseminated in accordance with this SORN. Finished intelligence products, and the information contained in those products, regardless of the original source system of that information, is also retained and disseminated in accordance with this SORN.

The previously issued Final Rule exempting portions of this system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements remains in effect.

This modified system will be included in DHS's inventory of record systems.

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. sec. 552a, the U.S.

Department of Homeland Security (DHS)/U.S. Customs and Border Protection (CBP) proposes to modify and reissue an existing DHS system of records titled, “DHS/CBP-024 CBP Intelligence Records System (CIRS) System of Records.”

The CBP Intelligence Records System (CIRS) system of records is owned by CBP’s Office of Intelligence (OI). CIRS contains information collected by CBP to support CBP’s law enforcement intelligence mission. This information includes raw intelligence information collected by CBP’s OI, public source information, and information initially collected by CBP pursuant to its immigration and customs authorities. This information is analyzed and incorporated into intelligence products. CBP currently uses the Analytical Framework for Intelligence (AFI) and the Intelligence Reporting System (IRS) information technology (IT) systems to facilitate the development of finished intelligence products. These products are disseminated to various stakeholders including CBP executive management, CBP operational units, various government agencies, and the Intelligence Community (IC).

CIRS is the exclusive CBP System of Records Notice for finished intelligence products and any raw intelligence information, public source information, or other information collected by CBP for an intelligence purpose that is not subject to an existing DHS SORN. Information collected by CBP for an intelligence purpose that is not covered by an existing DHS SORN and is not incorporated into a finished intelligence product is retained and disseminated in accordance with this SORN. In addition, finished intelligence products, and the information contained in those products, regardless of the original source system of that information, is retained and disseminated in accordance with this SORN. CIRS records were previously covered by the Automated Targeting System SORN and the Analytical Framework for Intelligence System SORN.

As part of the intelligence process, CBP investigators and analysts must review large amounts of data to identify and understand relationships between individuals,

entities, threats, and events to generate law enforcement intelligence products that provide CBP operational units with actionable information for law enforcement purposes. If performed manually, this process can involve hours of analysis of voluminous data. To automate and expedite this process, CBP uses several IT systems to allow for the efficient research and analysis of data from a variety of sources. Existing IT systems that CBP uses to analyze and produce intelligence information include AFI and IRS.

AFI is specifically designed to make the intelligence research and analysis process more efficient by allowing searches of a broad range of data through a single interface. AFI can also identify links (relationships) between individuals or entities based on commonalities, such as identification numbers, addresses, or other information. These commonalities in and of themselves are not suspicious, but in the context of additional information they sometimes help DHS agents and analysts to identify potentially criminal activity and identify other suspicious activities. These commonalities can also form the basis for a DHS-generated intelligence product that may lead to further investigation or other appropriate follow-up action by CBP, DHS, or other federal, state, or local agencies. DHS/CBP has published a Privacy Impact Assessment (PIA) for AFI, which is available on www.dhs.gov/privacy. A PIA for IRS is forthcoming.

CBP is updating and reissuing this existing system of records to provide additional transparency regarding the publicly available landowner records CBP receives from state and local jurisdictions or may access via a commercial data provider. Property records are publicly available and often searchable via online databases provided by local municipalities and counties and by commercial providers. As part of its border security mission, DHS/CBP requires accurate information about landowner information along the borders of the United States to seek expedited real estate Rights of Entry (ROE), Right of Way (ROW), and subsequent acquisition of land for the placement of proposed and approved border surveillance technology and infrastructure. DHS/CBP is clarifying that it

receives publicly available landowner information from local jurisdictions and commercial providers. CBP is also clarifying that individuals covered by the system may include individuals not implicated in activities in violation of laws enforced or administered by CBP but with pertinent knowledge of some circumstance of a case or record subject. This category was previously limited to only individuals with knowledge of narcotics trafficking or related activities. Additionally, DHS/CBP is modifying Routine Use "E" and adding Routine Uses "F" to conform to OMB Memorandum M-17-12. The previous Routine Use "F" has been renumbered as Routine Use "H," and the content of the previous Routine Use "G" has been modified to conform with the current DHS template. All subsequent Routine Uses have been renumbered to account for these changes. Additionally, this notice includes non-substantive changes to simplify the formatting and text of the previously published notice.

Individuals may request information about records pertaining to themselves stored in CIRS as outlined in the "Notification Procedure" section below. CBP reserves the right to exempt various records from release pursuant to exemptions 5 U.S.C. 552a(j)(2), (k)(1) and (k)(2) of the Privacy Act.

Consistent with DHS's information sharing mission, information stored in the DHS/CBP-024 CIRS 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/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 SORN.

The previously issued Final Rule exempting portions of this system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements remains in effect. 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. Similarly, the Judicial Redress Act (JRA) provides a statutory right to covered persons 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/CBP-024 Intelligence Records System (CIRS) System of Records.

In accordance with 5 U.S.C. 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: U.S. Department of Homeland Security (DHS)/U.S. Customs and Border Protection (CBP)-024 CBP Intelligence Records System (CIRS) System of Records.

SECURITY CLASSIFICATION: Unclassified, Sensitive, For Official Use Only, Law Enforcement-Sensitive, and Classified.

SYSTEM LOCATION: CBP maintains CIRS records at the CBP Headquarters in Washington, D.C. and field offices. CBP uses the Analytical Framework for Intelligence (AFI) and the Intelligence Reporting System (IRS) to facilitate the development of

finished intelligence products and maintain a repository of intelligence information records. Records may also be stored on paper within the Office of Intelligence (OI), the National Targeting Center, or in CBP field offices.

SYSTEM MANAGER: Assistant Commissioner for the Office of Intelligence, U.S. Customs and Border Protection, 1300 Pennsylvania Avenue N.W., Washington, D.C. 20229.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title II of the Homeland Security Act of 2002 (Pub. L. 107-296), as amended by the Intelligence Reform and Terrorism Prevention Act of 2004 (Pub. L. 108-458, 118 Stat. 3638); the Trade Facilitation and Trade Enforcement Act of 2015 (Pub. L. 114-125); the Tariff Act of 1930, as amended; the Immigration and Nationality Act (“INA”), 8 U.S.C. 1101, et seq.; the Implementing Recommendations of the 9/11 Commission Act of 2007 (Pub. L. 110-53); the Antiterrorism and Effective Death Penalty Act of 1996 (Pub. L. 104-132, 110 Stat. 1214); the SAFE Port Act of 2006 (Pub. L. 109-347); the Aviation and Transportation Security Act of 2001 (Pub. L. 107-71); 6 U.S.C. 202; and 6 U.S.C. 211.

PURPOSE(S) OF THE SYSTEM: This system of records describes CBP’s collection and consolidation of information from multiple sources, including law enforcement agencies and agencies of the U.S. Intelligence Community, in order to enhance CBP’s ability to: identify, apprehend, or prosecute individuals who pose a potential law enforcement or security risk; aid in the enforcement of the customs and immigration laws, and other laws enforced by DHS at the border; and enhance U.S. border security.

CBP maintains intelligence information to:

- (a) Support CBP’s collection, analysis, reporting, and distribution of law enforcement, immigration administration, terrorism, intelligence, and homeland security information in support of CBP’s law enforcement, customs and immigration, counterterrorism, national security, and other homeland

security missions.

- (b) Produce law enforcement intelligence reporting that provides actionable information to CBP's law enforcement and immigration administration personnel and to other appropriate government agencies.
- (c) Enhance the efficiency and effectiveness of the research and analysis process for DHS law enforcement, immigration, and intelligence personnel through information technology tools that provide for advanced search and analysis of various datasets.
- (d) Identify potential criminal activity, violations of federal law, and threats to homeland security; provide overall situational awareness for the CBP enterprise; to uphold and enforce the law; and to ensure public safety.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Categories of individuals covered by this system include the following:

1. Individuals (e.g., subjects, witnesses, associates, informants) associated with border security, immigration or customs enforcement, or other law enforcement investigations/activities conducted by CBP;
2. Individuals associated with law enforcement investigations or activities conducted by other federal, state, tribal, territorial, local, or foreign agencies when there is a potential nexus to national security, CBP's law enforcement responsibilities, or homeland security in general;
3. Individuals known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism;
4. Individuals involved in, associated with, or who have reported suspicious activities, threats, or other incidents reported by domestic and foreign government agencies, multinational or non-governmental organizations, critical infrastructure owners and operators, private sector entities and organizations, and individuals;

5. Individuals not implicated in activities in violation of laws enforced or administered by CBP, but with pertinent knowledge of some circumstance of a case or record subject. Such records may contain any information, including personal identification data, that may assist CBP in discharging its responsibilities generally (e.g., information which may assist in identifying and locating such individuals);
6. Individuals who are the subjects of or otherwise identified in classified or unclassified intelligence reporting received or reviewed by CBP OI;
7. Individuals identified in law enforcement, intelligence, crime, and incident reports (including financial reports under the Bank Secrecy Act and law enforcement bulletins) produced by DHS and other government agencies;
8. Individuals identified in U.S. visa, border, immigration, and naturalization benefit data, including arrival and departure data;
9. Individuals identified in DHS law enforcement and immigration records;
10. Individuals not authorized to work in the United States;
11. Individuals whose passports have been lost or stolen; and
12. Individuals identified in any publicly available or commercially available information source such as news reports, property records, and social media postings.

CATEGORIES OF RECORDS IN THE SYSTEM: Categories of records in this system include information collected by CBP for an intelligence purpose that is not covered by an existing DHS SORN and finished intelligence products. This information may include:

1. Biographic information (e.g., name, date of birth, Social Security number, alien registration number, citizenship/immigration status, passport information, addresses, phone numbers);

2. Records of immigration enforcement activities or law enforcement investigations/activities;
3. Information (including documents and electronic data) collected by CBP from or about individuals during investigative activities and border searches;
4. Records of immigration enforcement activities and law enforcement investigations/activities that have a possible nexus to CBP's law enforcement and immigration enforcement responsibilities or homeland security in general;
5. Law enforcement, intelligence, crime, and incident reports (including financial reports under the Bank Secrecy Act and law enforcement bulletins) produced by DHS and other government agencies;
6. U.S. visa, border, immigration, and naturalization benefit data, including arrival and departure data;
7. Terrorist watchlist information and other terrorism-related information regarding threats, activities, and incidents;
8. Lost and stolen passport data;
9. Records pertaining to known or suspected terrorists, terrorist incidents, activities, groups, and threats;
10. CBP-generated intelligence requirements, analysis, reporting, and briefings;
11. Information from investigative and intelligence reports prepared by law enforcement agencies and agencies of the U.S. foreign intelligence community;
12. Articles, public-source data (including information from social media), commercially available information, and other published information on individuals and events of interest to CBP;
13. Audio and video records retained in support of CBP's law enforcement, national security, or other homeland security missions;
14. Records and information from government data systems or retrieved from

commercial data providers in the course of intelligence research, analysis, and reporting, including records of property ownership;

15. Reports of suspicious activities, threats, or other incidents generated by CBP or third parties;

16. Additional information about confidential sources or informants; and

17. Metadata, which may include but is not limited to transaction date, time, location, and frequency.

RECORD SOURCE CATEGORIES: Federal, state, local, territorial, tribal, or other domestic agencies, foreign agencies, multinational or non-governmental organizations, critical infrastructure owners and operators, private sector entities and organizations, individuals, commercial data providers, and public sources such as social media, news media outlets, and the Internet.

CBP will abide by the safeguards, retention schedules, and dissemination requirements of DHS source system SORNs to the extent those systems are applicable and the information is not incorporated into a finished intelligence product. For additional information, please see the Privacy Impact Assessment for the Analytical Framework for Intelligence and the forthcoming Privacy Impact Assessment for the Intelligence Reporting System.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES: Source data are to be handled consistent with the published system of records notice as noted in “Source Category Records.” Source data that is not part of or incorporated into a finished intelligence product, a response to a request for information (RFI), project, or the index shall not be disclosed external to DHS. The routine uses below apply only to finished intelligence products, responses to RFIs, projects, and responsive compilations of the index and only as explicitly stated in each routine use.

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 or 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 Offices of the U.S. 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 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 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 a federal, state, territorial, tribal, local, international, or foreign government agency or entity for the purpose of consulting with that agency or entity: (1) To assist in making a determination regarding redress for an individual in connection with the operations of a DHS component or program; (2) for the purpose of verifying the identity of an individual seeking redress in connection with the operations of a DHS component

or program; or (3) for the purpose of verifying the accuracy of information submitted by an individual who has requested such redress on behalf of another individual.

J. To a former employee of DHS, in accordance with applicable regulations, for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes when the Department requires information or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

K. To an appropriate federal, state, local, tribal, foreign, or international agency, if the information is relevant and necessary to the 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 and when disclosure is appropriate to the proper performance of the official duties of the person receiving the information.

L. To appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations 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 risk.

M. 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.

N. To a federal, state, tribal, local, or foreign government agency or organization, or international organization, lawfully engaged in collecting law enforcement intelligence information, whether civil or criminal, or charged with investigating, prosecuting, enforcing, or implementing civil or criminal laws, related rules, regulations or orders, to enable these entities to carry out their law enforcement responsibilities, including the collection of law enforcement intelligence.

O. To appropriate federal, state, local, tribal, 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, license, or treaty when DHS determines that the information would assist in the enforcement of civil, criminal, or regulatory laws.

P. To third parties during the course of an investigation by DHS, a proceeding within the purview of the immigration and nationality laws, or a matter under DHS's jurisdiction, 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.

Q. 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.

R. To federal and foreign government intelligence or counterterrorism agencies when DHS reasonably believes there to be a threat or potential threat to national or international security for which the information may be useful in countering the threat or

potential threat, when DHS reasonably believes such use is to assist in anti-terrorism efforts, and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure.

S. To an organization or individual 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, to the extent the information is relevant to the protection of life or property and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure.

T. To the Department of State in the processing of petitions or applications for benefits under the Immigration and Nationality Act, and all other immigration and nationality laws including treaties and reciprocal agreements.

U. To appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations, with the approval of the Chief Privacy Officer, when DHS is aware of a need to use relevant data for purposes of testing new technology and systems designed to enhance national security or identify other violations of law.

V. 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 a clearly unwarranted invasion of personal privacy.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: DHS/CBP 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/CBP may retrieve records by personal identifiers such as but not limited to name, alien registration number, phone number, address, Social Security number, or passport number. DHS/CBP may retrieve records by non-personal information such as transaction date, entity/institution name, description of goods, value of transactions, and other information.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF

RECORDS: To the extent that CBP accesses and incorporates information from other DHS systems of records as sources of information for finished intelligence products, CBP will abide by the safeguards, retention schedules, and dissemination requirements of those underlying source systems of record. For additional information, please see the Privacy Impact Assessment for the Analytical Framework for Intelligence and the forthcoming Privacy Impact Assessment for the Intelligence Reporting System.

Consistent with the DHS N1-563-07-016 records schedule, CBP will retain information consistent with the same retention requirements of the DHS Office of Intelligence and Analysis:

1. Dissemination Files and Lists: CBP will retain finished and current intelligence report information distributed to support the Intelligence Community, DHS Components, and federal, state, local, tribal, and foreign Governments and includes contact information for the distribution of finished and current intelligence reports for two (2) years.
2. Raw Reporting Files: CBP will retain raw, unevaluated information on threat reporting originating from operational data and supporting documentation that are not covered by an existing DHS system of records for thirty (30) years.
3. Finished Intelligence Case Files: CBP will retain finished intelligence and associated background material for products such as Warning Products

identifying imminent homeland security threats, Assessments providing intelligence analysis on specific topics, executive products providing intelligence reporting to senior leadership, intelligence summaries about current intelligence events, and periodic reports containing intelligence awareness information for specific region, sector, or subject/area of interest as permanent records and will transfer the records to the National Archives and Records Administration (NARA) after twenty (20) years.

4. Requests for Information/Data Calls: CBP will retain requests for information and corresponding research, responses, and supporting documentation for ten (10) years.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL 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 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: The Secretary of Homeland Security has exempted this system from the notification, access, and amendment procedures of the Privacy Act, and the Judicial Redress Act if applicable, 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 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 CBP Freedom of Information Act (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 FOIA Officer, U.S. Department of Homeland Security, Washington, D.C. 20528. Even if neither the Privacy Act nor the Judicial Redress Act provide a right of access, certain records about you may be available under the Freedom of Information Act.

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 FOIA Officer, <http://www.dhs.gov/foia> or (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.

CONTESTING RECORD PROCEDURES: For records covered by the Privacy Act or covered JRA records, see “Record Access Procedures” above. For records not covered by the Privacy Act or JRA, individuals may submit an inquiry to the DHS Traveler Redress Inquiry Program (DHS TRIP) at <https://www.dhs.gov/dhs-trip> or the CBP INFO CENTER at www.help.cbp.gov or (877) 227-5511 (international callers may use (202) 325-8000 and TTY users may dial (866) 880-6582).

NOTIFICATION PROCEDURES: See “Record Access Procedures.”

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) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5) and (e)(8); (f); and (g). Additionally, the Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(k)(1) and (k)(2), has exempted this system from the following provisions of the Privacy Act, 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), and (e)(4)(H); (e)(4)(I), and (f). When this system receives a record from another system exempted in that source system under 5 U.S.C. 552a(k)(1); (k)(2); or (j)(2), DHS will claim the same exemptions for those records that are claimed for the original primary systems of records from which they originated and claims any additional exemptions set forth here.

HISTORY: 82 Fed. Reg. 44198 (September 21, 2017).

Constantina Kozanas,

Chief Privacy Officer,

U.S. Department of Homeland Security.

[FR Doc. 2020-27446 Filed: 12/11/2020 8:45 am; Publication Date: 12/14/2020]