DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS-2017-0001]

Privacy Act of 1974; System of Records

AGENCY: Department of Homeland Security, Privacy Office.

ACTION: Notice of New 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/Immigration and Customs Enforcement-016 FALCON Search and Analysis System of Records." FALCON Search and Analysis is a consolidated information management system that enables ICE law enforcement and homeland security personnel to search, analyze, and visualize volumes of existing information in support of ICE's mission to enforce and investigate violations of U.S. criminal, civil, and administrative laws. Additionally, elsewhere in the Federal Register, 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 because of the law enforcement sensitivity of the data contributed to and produced within the system of records. This newly established system 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-2017-0001 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.

FOR FURTHER INFORMATION CONTACT: For general questions, please contact: Amber Smith (202) 732-3300, Privacy Officer, U.S. Immigration and Customs Enforcement. For privacy questions, please contact: Jonathan R. Cantor, (202) 343-1717, Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528-0655.

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. Immigration and Customs Enforcement (ICE) proposes to establish a new DHS system of records titled, "DHS/Immigration and Customs Enforcement-016 FALCON Search and Analysis System of Records."

U.S. Immigration and Customs Enforcement (ICE) is establishing a consolidated information management system to enable its personnel to search, analyze, and visualize volumes of existing information in support of ICE's mission to enforce and investigate violations of U.S. criminal, civil, and administrative laws. The FALCON Search and Analysis (FALCON-SA) System of Records describes the operation of an ICE information technology system of the same name, which is owned by ICE's Office of Homeland Security Investigations (HSI). This

system contains a repository of data that is ingested on a routine or ad hoc basis from other existing sources, and an index created from that data to be used for research and analysis in support of ICE HSI's law enforcement mission. FALCON-SA incorporates tools that allow the data to be queried, analyzed, and presented in a variety of formats that can help illuminate relationships among the various data elements. The purpose of FALCON-SA is to help ICE HSI personnel conduct research and analysis using advanced analytic tools in support of their law enforcement mission.

This system of records ingests and aggregates data from a number of interfaces that fall under the FALCON umbrella, including the FALCON-Tip Line, FALCON-Data Analysis & Research for Trade Transparency System (DARTTS), and FALCON-Roadrunner. All data aggregated from these interfaces, and user access is controlled through a combination of data tagging, access control lists, and other technologies. Using a central data store for FALCON data eliminates the need for multiple copies of the data and streamlines the application of many security and privacy controls. Only data accessed via FALCON-SA is covered by the DHS/ICE-016 FALCON-SA System of Records Notice (SORN). However, the other interfaces are covered by other ICE SORNs, as specified in the System Location section of the SORN. Separate SORNs are appropriate because the data, purposes, and routine uses differ depending on which FALCON interface is being used.

FALCON-SA Data

Information included in FALCON-SA is ingested either on a routine or ad hoc basis. Routine ingests are regular updates to datasets that originate from other Government (typically ICE or DHS) data systems. A list of routine ingests into the FALCON general data storage

environment that is accessible via FALCON-SA is available in the FALCON-SA Privacy Impact Assessment at www.dhs.gov/privacy.

Ad hoc ingests are user-driven ingests of particular data that may be relevant to a given user or group's investigative or analytical project in FALCON-SA. The nature of the data in ad hoc ingests varies from data collected from a commercial or public source (e.g., Internet research or from a commercial data service), to public reports of law enforcement violations or suspicious activity (tips), to digital records seized or subpoenaed during an investigation. All ad hoc ingests are tagged by the FALCON-SA user with the appropriate category description, and that tag controls the retention policy for that data. The ad hoc ingest category description list is included in the FALCON-SA Privacy Impact Assessment at www.dhs.gov/privacy.

FALCON-SA records may include some or all of the following types of personally identifiable information: identifying and biographic data such as name and date of birth; citizenship and immigration data; border crossing data; customs import-export history; criminal history; contact information; criminal associates; family relationships; photographs and other media; and employment and education information.

FALCON-SA also contains an index, which is a numerical and alphabetical list of every word or string of numbers/characters found in the FALCON-SA database, with a reference to the electronic location where the corresponding source record is stored. FALCON-SA uses this index to conduct searches, identify relationships and links between records and data, and generate visualizations for analytic purposes. FALCON-SA also contains metadata that is created when the myriad sources of data are ingested. The metadata is used to apply access controls and other system rules (such as retention policies) to the contents of FALCON-SA. The metadata

also provides important contextual information about the date the information was added to FALCON-SA and the source system where the data originated.

The data sets in FALCON-SA include tips submitted to ICE either through an online form on the ICE website or by calling the HSI Tip Line. These tips are created electronically using the FALCON-Tip Line interface, or may be manually entered by HSI's Cyber Crimes Center when the tips pertain to child exploitation crimes. Once HSI adjudicates the tips for action, the tips are then accessible to all HSI users via the FALCON-SA interface.

Uses of FALCON-SA

ICE HSI agents, criminal research specialists, and intelligence analysts query FALCON-SA for a variety of purposes: to conduct research that supports the production of law enforcement intelligence products; to provide lead information for investigative inquiry and follow-up; to assist in the conduct of ICE criminal, civil, and administrative investigations; to assist in the disruption of terrorist or other criminal activity; and to discover previously unknown connections among existing ICE investigations. These queries can be saved in FALCON-SA to eliminate the need to recreate them each time a user logs on.

Strong access controls and a robust audit function ensure that ICE's use of the system is predicated on homeland security, law enforcement, and law enforcement intelligence activities. This requirement is enforced by a governance group composed of leadership from HSI with oversight by ICE's legal, privacy and civil liberties offices.

While ICE previously relied on the DHS/ICE-006 ICE Intelligence Records System (IIRS) SORN, last published at 75 FR 9233 (Mar. 1, 2010), to maintain FALCON-SA records, it was determined that a separate system of records notice will provide greater transparency and

allow ICE to more accurately describe the records accessible via FALCON-SA. FALCON-Tip Line records were previously covered by the DHS/ICE-007 Alien Criminal Response Information Management (ACRIMe) SORN, but the FALCON-SA SORN will now cover those records instead. This change is due to the fact that Tip Line records have migrated out of the ACRIMe system into the FALCON environment and that once created, the official repository for FALCON-Tip Line records is the FALCON general data storage environment.

This SORN will cover data that is accessible via FALCON-SA's user interface only, and does not cover data that is accessed via other FALCON interfaces, such as Roadrunner and DARTTS, which are covered by the DHS/ICE-005 Trade Transparency and Analysis Records (TTAR) SORN.

Additional information about FALCON-SA can be found in the Privacy Impact Assessments published for FALCON-SA and FALCON-Tip Line, available at http://www.dhs.gov/privacy-documents-ice.

Consistent with DHS's information sharing mission, information stored in the DHS/ICE-016 FALCON-SA 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, ICE 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. Additionally, and 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/ ICE-016 FALCON-SA 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: DHS/ICE-016 FALCON-Search and Analysis (FALCON-SA)

SECURITY CLASSIFICATION: Unclassified; Law Enforcement Sensitive; and For Official Use Only

SYSTEM LOCATION: DHS/ICE maintains records in DHS data centers. This SORN applies to all records available to users through the FALCON-SA interface. This SORN also applies to all records created through the FALCON-Tip Line interface.

SYSTEM MANAGER(S): Assistant Director for Information Management Directorate, Homeland Security Investigations, U.S. Immigration and Customs Enforcement, 500 12th Street, SW, Washington, D.C. 20536.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 8 U.S.C. 1103, 1105; 8 U.S.C. 1225(d)(3) and (d)(4)(A); 8 U.S.C. 1324a(e)(2)(C); 8 U.S.C. 1357; 8 U.S.C. 1360(b); 18 U.S.C. 2703; 19 U.S.C. 1509; 19 U.S.C. 1589a; 19 U.S.C. 1628; 21 U.S.C. 967; and 50 U.S.C. 2411(a).

PURPOSE(S) OF THE SYSTEM: The purpose of this system of records is to permit ICE law enforcement and homeland security personnel to search, aggregate, analyze, and visualize volumes of existing information in support of ICE's mission to enforce and investigate violations of U.S. criminal and administrative laws. FALCON-SA allows ICE HSI agents, criminal research specialists, and intelligence analysts to conduct research in order to produce law enforcement intelligence, provide lead information for investigative inquiry and follow-up, assist in the conduct of ICE investigations and the disruption of criminal (including terrorist) activity, and discover previously unknown connections among ICE investigations.

This system of records also supports the operation of the agency's Tip Line to collect, analyze, and act on information volunteered by the public and other sources concerning suspicious and potentially illegal activity.

This system of records also supports the identification of potential criminal activity, immigration violations, and threats to homeland security. The system is used to uphold and enforce the law, and to ensure public safety.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

1) Individuals who owned, had custody of, or arranged for the import or export of property that is seized by ICE or U.S. Customs and Border Protection (CBP);

2) Individuals identified in TECS subject records and investigative records created by ICE and CBP, including violators or suspected violators of laws enforced or administered by ICE and CBP; individuals arrested by ICE and CBP for violations of law; witnesses associated with ICE and CBP enforcement actions; persons who own or operate businesses, property, vehicles, or other property that is in a TECS subject record; and individuals applying for a license issued by DHS or for which DHS conducts a background investigation in support of the licensing agency;

3) Subjects of administrative actions by ICE, such as individuals who are the subject or proponent of a continued presence parole application under the Immigration and Nationality Act;

4) Subjects of ICE threat assessments such as gang members;

5) Aliens arrested, detained, and/or removed by ICE, or issued a notice to appear in immigration court, under the Immigration and Nationality Act;

6) Aliens who are the subject of an ICE immigration detainer or request for notification;

7) ICE personnel or personnel from partner law enforcement agencies who are mentioned in significant incident reports that concern law enforcement (LE) operations, injuries to law enforcement personnel, or other significant incidents reported within ICE;

8) Individuals who are associated with an ICE investigation, have provided information to ICE during an investigation, or whose data is part of records or other materials collected, compiled, or seized during an investigation, including victims, witnesses, associates, and sources;

9) Individuals alleged to be involved in suspicious or illegal activity, and the

individuals reporting such activity to ICE;

10) Specially Designated Nationals, as defined by 31 CFR 500.306;

11) Individuals identified on other denied parties or screening lists; and

12) Government personnel associated with official requests by another agency for ICE assistance, or associated with any of the foregoing categories of individuals.

CATEGORIES OF RECORDS IN THE SYSTEM:

1) Biographic and other identifying information, including names; dates of birth; places of birth; Social Security numbers (SSN); Tax Identification Numbers (TIN); Exporter Identification Numbers (EIN); passport information (number and country of issuance); citizenship; nationality; location and contact information (e.g., home, business, and email addresses and telephone numbers); and other identification numbers (e.g., Alien Registration Number, driver's license number).

2) Financial data, including data reported pursuant to the Bank Secrecy Act (e.g., certain transactions over $10,000) and other financial data obtained via official investigations, legal processes, or legal settlements. Financial data includes, but is not limited to, bank account numbers, transaction numbers, and descriptions or value of financial transactions.

3) Licensing information related to applications by individuals or businesses to hold or retain a customs broker's license, operate a customs-bonded warehouse, or be a bonded carrier or bonded cartman.

4) Various internal operational reports, including reports of significant incidents and operations; reports concerning prospective enforcement activity; requests for assistance from other law enforcement agencies; agency intelligence reports; and reports of third-agency visits to ICE detention facilities.

5) Law enforcement records, including TECS subject records and investigative records related to an ICE or CBP law enforcement matter, information obtained from the U.S. Department of the Treasury's Specially Designated Nationals List, visa security information, and other trade-based and financial sanction screening lists. Law enforcement data includes, but is not limited to, names; aliases; business names; addresses; dates of birth; places of birth; citizenship; nationality; passport information; SSNs; TINs; driver's license numbers; and vehicle, vessel, and aircraft information.

6) Reports of fines, penalties, forfeitures, and seizure incidents.

7) Records of call transactions and subscriber information obtained during the course of an ICE criminal investigation.

8) Tips concerning illegal or suspicious activity from the public and other law enforcement agencies.

9) Continued presence parole application records.

10) Open source information - news articles or other data available to the public on the Internet or in public records, including publicly available information from social media.

11) Commercially available data - public and proprietary records available for a subscription.

12) Cargo and border crossing data – inbound/outbound shipment records and border crossing information from CBP's Automated Targeting System. NOTE: Passenger Name Record (PNR) data may not be uploaded into this system of records.

13) Criminal information, including lookouts, warrants, criminal history records, and other civil or criminal investigative information provided by other law enforcement agencies.

14) Information from foreign governments or multinational organizations such as

INTERPOL or Europol – including criminal history; immigration data; passenger, vehicle, vessel entry/exit data; passport information; vehicle, vessel, and licensing records; shipment records; telephone records; intelligence reports; investigative leads and requests; and wants, warrants, and lookouts.

15) Finished intelligence reports from DHS or other agencies.

16) Evidentiary information concerning evidence seized or otherwise lawfully obtained during the course of an ICE investigation, including business records, third-agency records, public records (courts, etc.), transcripts of interviews/depositions, or materials seized or obtained via subpoena or other lawful process.

17) Trade analysis data, including trade identifier numbers (e.g., for manufacturers importers, exporters, and customs brokers) and bill of lading data (e.g., consignee names and addresses, shipper names and addresses, container numbers, carriers); other financial data required for the detection and analysis of financial irregularities and crimes.

18) Tip data concerning child exploitation violations, such as the biographical data of the suspect or the suspect's online identity information (user ID). Internet Service Provider data, domain name, credit card number and Internet Protocol (IP) address, Internet subscriber data (name, subscriber number, billing address, IP address, payment method, and email addresses), a log of subscriber activity, or other information such as motor vehicle data, SSN, and other information collected during the course of vetting the tip from sources such as Government databases, and open source and commercially-available data, as previously described.

RECORD SOURCE CATEGORIES: Records are obtained from other ICE and DHS record systems as well as records or information from other agencies, DHS partners, and the public. Public records and commercial data may also be added to the system.

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 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. 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 the security or confidentiality of information in the system of records has been compromised;

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

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

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

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

H. To Federal, State, local, tribal, territorial, foreign or international agencies, if the information is relevant and necessary to a requesting agency's decision concerning the hiring or

retention of an individual; the issuance, grant, renewal, suspension, or revocation of a security clearance, license, contract, grant, or other benefit; or if the information is relevant and necessary to a DHS decision concerning the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit.

I. To Federal, State, local, tribal, territorial, international, or foreign criminal, civil, or regulatory law enforcement authorities when the information is necessary for collaboration, coordination, and de-confliction of investigative matters, prosecutions, and/or other law enforcement actions to avoid duplicative or disruptive efforts and to ensure the safety of law enforcement officers who may be working on related law enforcement matters.

J. To international, foreign, intergovernmental, and multinational government agencies, authorities, and organizations in accordance with law and formal or informal international arrangements.

K. To Federal, State, local, tribal, territorial, or foreign government agencies or organizations, or international organizations, lawfully engaged in collecting law enforcement intelligence, whether civil or criminal, to enable these entities to carry out their law enforcement responsibilities, including the collection of law enforcement intelligence.

L. 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.

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 to the proper performance of the official duties of the officer making the disclosure.

N. To other Federal law enforcement agencies, the disclosure of call detail records to coordinate criminal investigations, specifically to assist in the identification of investigations that may be related, as well as the deconfliction of cases.

O. 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/ICE 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: Records may be retrieved by name or other personal identifier.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: The retention period for information contained in FALCON-SA varies depending on the type of data. Routinely ingested DHS-owned data is retained in accordance with the approved record retention schedule of the source system. Data uploaded to FALCON-SA in an ad hoc manner is associated with a case file number, to the extent possible, and retained consistent with the retention of the

case file. When there is no case file number, the data is retained for 20 years. FALCON-SA metadata and index data are retained for the same length of time as the record or data element they originate from or describe.

FALCON-SA is the official repository for tip information at ICE and does not obtain these records from another internal database source. ICE records created via the FALCON-Tip Line application are fed into FALCON-SA's general data storage environment thereafter. Other tip information may be entered into FALCON-SA manually by a specialized unit within ICE when the tips pertain to child exploitation crimes. Tip Line records will be retained for ten (10) years from the date of the tip. Tip records concerning child exploitation crimes will be retained for 75 years.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: DHS/ICE safeguards records in this system according to applicable rules and policies, including all applicable DHS automated systems security and access policies. ICE 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 and ICE will consider individuals' 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 U.S.

Immigration and Customs Enforcement Freedom of Information Act (FOIA) Officer, whose contact information can be found at http://www.dhs.gov/foia under "FOIA Contact 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 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. 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.

CONTESTING RECORD PROCEDURES: Individuals who wish to contest the accuracy of records in this system of records should submit these requests to the ICE Privacy & Records Office. Requests must comply with verification of identity requirements set forth in Department of Homeland Security Privacy Act regulations at 6 CFR 5.21(d). Please specify the nature of the complaint and provide any supporting documentation. By mail (please note substantial delivery delays exist): ICE Privacy & Records Office, 500 12th Street, SW, Mail Stop 5004, Washington D.C., 20536. By email: ICEPrivacy@ice.dhs.gov. Please contact the Privacy & Records Office with any questions about submitting a request or complaint at 202-732-3300 or ICEPrivacy@ice.dhs.gov.

NOTIFICATION PROCEDURES: See "Record Access procedure."

EXEMPTIONS PROMULGATED FOR THE SYSTEM: The Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(j)(2) and (k)(2), has exempted this system from the following provisions of the Privacy Act: 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); and (g).

When FALCON-SA receives a record from another system that is exempt from the Privacy Act, DHS will claim the same exemptions as are claimed for the original system of records from which the record originated and also claims any additional exemptions set forth here.

Dated: May 1, 2017.

Jonathan R. Cantor,

Acting Chief Privacy Officer,

Department of Homeland Security.

[FR Doc. 2017-09025 Filed: 5/3/2017 8:45 am; Publication Date: 5/4/2017]