Privacy Impact Assessment
for the

FALCON Search & Analysis System

DHS/ICE/PIA-032

February 1, 2012

Contact Point
James Dinkins
Executive Associate Director
Homeland Security Investigations
U.S. Immigration & Customs Enforcement
(202) 732-5100

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

U.S. Immigration and Customs Enforcement (ICE), a component agency within the Department of Homeland Security (DHS), is establishing a consolidated information management system called FALCON Search & Analysis System (hereafter, FALCON-SA). This system 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 and administrative laws. ICE agents, criminal research specialists, and intelligence analysts use FALCON-SA to conduct research that support the production of law enforcement intelligence products, provide lead information for investigative inquiry and follow-up, assist in the conduct of ICE criminal and administrative investigations, assist in the disruption of terrorist or other criminal activity, and discover previously unknown connections among existing ICE investigations. ICE's use of the system is always predicated on homeland security, law enforcement, and intelligence activities. FALCON-SA is an internal system used only by ICE.

In order to mitigate privacy and security risks associated with the deployment of FALCON-SA, ICE has built technical safeguards into the system and developed a governance process that includes the operational components of ICE Homeland Security Investigations, the oversight functions of the ICE Privacy Office, Office Principal Legal Advisor, and Office of the Chief Information Officer.

This Privacy Impact Assessment (PIA) is necessary because FALCON-SA accesses and stores personally identifiable information (PII) retrieved from DHS, other government agency, and commercially available databases. It is also necessary to provide public notice of the existence of FALCON-SA and to publicly document the privacy protections that are in place for the system.

Overview

ICE developed FALCON-SA to enhance ICE's ability to identify, apprehend, and prosecute individuals who violate criminal and administrative laws enforced by ICE.[1] FALCON-SA augments ICE's ability to review and develop information about persons, organizations, events, and locations by ingesting and creating an index of the data from other existing operational government data systems and providing ICE agents, criminal research specialists, and intelligence analysts with different tools that visualize the data to help identify relationships. FALCON-SA supports the investigative work of ICE Homeland Security Investigations (HSI) agents and criminal research specialists by allowing them to search, review, upload, and analyze data pertinent to an investigative lead or an ongoing case. Examples of the outcomes of an HSI agent's work in FALCON-SA may be to find or validate a new investigative lead, to identify a connection between two previously unconnected ICE investigations, or to create a chart that visualizes the connections and relationships among various persons and enterprises in a complex criminal case. FALCON-SA also allows ICE intelligence analysts to conduct analysis in support of ICE's mission. FALCON-SA is a tool that allows users to search and analyze the ingested data and to identify connections. ICE analysts use the results of their analysis in FALCON-SA to generate tactical, operational, and strategic law enforcement intelligence products (hereinafter referred to as "finished intelligence products"). Occasionally the visualizations will be exported from FALCON-SA to a finished intelligence product, but only with supervisory approval. Finished intelligence products better inform the consumers of these products, which include DHS and ICE leadership, agents, officers, and employees,

[1] FALCON-SA is ultimately intended to replace ICE's Law Enforcement Intelligence Fusion System (IFS). PIA: DHS/ICE/PIA-007 (Nov. 17, 2008).

about the overall impact of ICE law enforcement operations, criminal trends and tactics, emerging threats, resource needs, and strategic goals and objectives.

FALCON-SA assists the human evaluation and decision-making process and helps reduce human error and analytic uncertainty by presenting information already available to the user in a common sense fashion. The data that the system contains is obtained from various DHS databases, as well as other sources that are appropriate and lawful sources of information for HSI's investigative and law enforcement mission. The Appendix to this PIA describes the data that is available in FALCON-SA, the specific sources, and how it is ingested and updated. FALCON-SA is being designed and developed in an iterative, incremental fashion. As the system evolves to include new classes of data and new functionality, this PIA and its Appendix will be updated.

System Functions, Data, and Structure

FALCON-SA aggregates data from various sources and allows users to visualize and share the data in analytically useful ways. For example, the system can organize information temporally or geographically or it can present a chart showing relational links between individuals and/or organizations whose data is stored in the system. These visualizations reflect the content of the underlying source data and allow the user to identify links or connections that may have been previously unknown or to quickly search data that previously was difficult to access because, for example, in the source system it was in a free form text field but in FALCON-SA it is in a searchable index. The visualizations are only maintained so long as the data in the ingested source system remains. If the source system deletes a record, the record will no longer be available to the user for a particular visualization. Users can also share the analytical data and results with limited numbers of other users, or with the FALCON-SA community as a whole.

Every FALCON-SA user has private "space" within the system where they conduct their analysis. This space is called a virtual domain, and essentially consists of a home page for the user where they create a project in support of an investigation or other assignment. Users are likely to have multiple projects open at the same time to support the various assignments and cases they are working. Users must name the project and, by policy, users are required to use the relevant ICE case number if one has been assigned. After creating the project, the user may perform the following actions:

- Upload records or input data relevant to the project (referred to as *ad hoc* data);
- Create, conduct, and save searches of any records/data stored in the project and other data published in FALCON-SA to which the user has access privileges;
- Conduct analysis of the data using the visualization tools in FALCON-SA;
- Save visualizations created using the system tools;
- Grant other users rights to view the project, including the uploaded records/data, saved searches, and visualizations;
- Publish the uploaded records/data or visualizations to other users in FALCON-SA; and
- Extract visualizations into another program, such as Microsoft PowerPoint.

As described in more detail below, the system or ICE policy may require users to obtain supervisory review and/or approval for some or all of these actions.

System Data

Through its source systems, FALCON-SA contains information on individuals who have had previous encounters with DHS of a law enforcement nature, such as during a DHS investigation or during the inspection process at a port of entry. As FALCON-SA evolves, the population of individuals on whom data is maintained will change and this PIA will be updated accordingly. The addition of future datasets and populations of individuals is overseen by an internal ICE governance process (described in more detail below), which will consider the legal and privacy issues raised by the inclusion of other populations into this system given its purpose and ICE's legal authorities. The specific PII elements in FALCON-SA concerning any particular individual vary depending on the source records about the individual that have been ingested. Generally, FALCON-SA records (whether from routine or *ad hoc* sources, or both) may include some or all of the following types of PII: identifying and biographic data, citizenship and immigration data, customs import-export history, criminal history, contact information, criminal associations, family relationships, employment, military service, education and other background information. This PII is necessary to accomplish the primary purpose of the system, which is to search, 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. The system's tools use the PII to conduct the analysis and visualize for the system user how individuals, events, or entities might be connected.

FALCON-SA contains a database consisting of data ingested on a routine or *ad hoc* basis from other existing sources, and an index created from that data. The system routinely ingests data from other ICE, DHS, or government data systems whose data is owned by ICE or has been identified by ICE as relevant and necessary to the ICE mission. FALCON-SA also permits users to upload data on an *ad hoc* basis in accordance with ICE policy. Users are authorized to upload records and information which are pertinent to the particular project in FALCON-SA they are working in, e.g., an investigation or an analysis project. Users are not permitted to upload extraneous materials or records that are not related to their official duties and assignments. Supervisory oversight of the *ad hoc* upload process helps to ensure users do not upload inappropriate or non-pertinent material. These routine and *ad hoc* ingests are further described in the Appendix to this PIA.

The FALCON-SA index is a numerical and alphabetical list of every word or string of numbers/characters in the FALCON-SA database with a reference to the electronic location where the corresponding source record in FALCON-SA is stored. FALCON-SA uses the index to conduct efficient searches, and identify relationships and links between records and data, and to generate visualizations of the data for analytical purposes.

FALCON-SA also captures metadata (i.e., data about data) for the data that is routinely ingested by it. Users are required to create metadata on data ingested into the database on an *ad hoc* basis. Metadata is used by the system to apply access and other system rules to records and data. Metadata is also used by the FALCON-SA users to assess the quality of the data they are viewing by providing the user more context about when the information was included in the system and the source of the information.

Visualizations are created and used to illustrate how individuals, entities, groups, incidents or activities relevant to the investigation or analysis are connected. In circumstances defined by ICE policy, FALCON-SA users may extract the visualizations from FALCON-SA and place them in another application, such as PowerPoint, for authorized use outside the system. Visualizations may need to be extracted during the course of an investigation or project for various purposes, such as to attach to reports or presentations, and for case management to include in case files, but can only be done with supervisory approval. When a visualization is extracted, the underlying source records are not extracted. Users may also create and save complex search queries within the FALCON-SA system. This prevents the user from having to re-enter search queries each time they logon to FALCON-SA. This is particularly useful for

longer-term analytical projects and investigations, when the results of the query are expected to be valuable for ongoing analysis or incorporation into visualizations.

Sharing of Data and Visualizations Within the System

FALCON-SA facilitates the sharing of data and visualizations with other users to help improve and expedite the analytical and investigative process. A key system function that facilitates sharing is the ability of users to upload data and records on an *ad hoc* basis. This allows users to identify relevant material to an investigation or analysis and, with supervisory approval, include it in a project within their virtual domain. *Ad hoc* data is input into FALCON-SA in two ways: by a user's upload of an electronic copy of a record, or by a user's manual entry of a particular piece of data, such as a date of birth or known alias for an individual. Because of the broad-ranging nature of law enforcement investigations and law enforcement intelligence work, it is not possible or advisable for every potentially useful data source to be ingested into FALCON-SA to support ICE's work. By allowing user-driven *ad hoc* uploads of data, with appropriate oversight and controls, the efficiency of investigations and analyses is greatly improved and collection of PII is minimized.

For example, during the course of a criminal investigation, HSI agents may obtain records and information from various outside sources during interviews and searches, or in response to subpoenas. Information that is pertinent to the investigation is appropriate to be uploaded into the corresponding project for that case in FALCON-SA.[2] Including this data in FALCON-SA will allow the agents to easily access, analyze, and share the data with each other, other members of their unit, and their supervisor(s). When data is uploaded into the FALCON-SA system by an HSI agent, the user is required to assign the appropriate case number to that data, thereby connecting it in the system to his/her investigation. A supervisor must always approve the upload of *ad hoc* data into FALCON-SA, to ensure the data is permitted by policy and otherwise appropriate to include in the system.

Visualizations created in or *ad hoc* data that is uploaded to a project in a user's virtual domain may be shared with other FALCON-SA users in two ways. First, the project owner may grant any other user privileges to view the data/visualization in the project. Those privileges are limited to view-only and do not permit other users to search, modify, or analyze that data using the FALCON-SA visualization tools. Second, the user may elect to publish the data to the system. The user can publish the data to one, several, or all FALCON-SA users. Once published, any users that have privileges to the data can search, modify, or analyze the data in FALCON-SA. Publication of any data or visualizations must be approved by a supervisor in advance.

System Users

FALCON-SA will be used by ICE HSI agents, criminal research specialists, and analysts in HSI headquarters and field offices, as well as HSI offices in U.S. embassies and consulates abroad. Other government agency personnel assigned to ICE HSI or to an ICE-led task force may also be granted access, as well as HSI contractors with a documented need to know. ICE grants access only to those who require access to the functionality and data in FALCON-SA in the performance of their official duties.

Based on their supervisory or non-supervisory status, individuals will be assigned one of two basic user roles: General User and Supervisor. General Users have the ability to search, review, upload,

[2] Uploading a copy of these records and information into FALCON-SA does not negate the requirement that the agents include the information in other appropriate ICE recordkeeping systems, such as the official case file.

and analyze data; create and store searches and visualizations; and grant other users access privileges to data they upload and searches/visualizations they create. Supervisors have all privileges of a General User, plus additional privileges related to overseeing the use of the system by General Users to ensure compliance with relevant laws and policies, and this PIA. Supervisors will, for example, have privileges to view the system audit trails for General Users, to review and approve uploads of *ad hoc* data, to access the virtual domains and projects of their staff, and to approve publication of any data, searches, or visualizations to the system. In addition, there is the system administrator role to ensure the system runs properly.

User privileges are customized beyond the user role initially assigned at account creation. For example, as a member of an investigative task force an ICE agent may be given privileges to access uploaded records seized during a search conducted by the task force. Because of investigative sensitivities related to the ongoing case, the task force does not make these records widely available to other FALCON-SA users. Privileges to access these types of records would be assigned on a user-by-user basis by the uploading user or a supervisor. A user can also control the ability of other users to access projects and materials (data/visualizations) within projects in the user's virtual domain.

Governance, Auditing, and Other Privacy Controls

To ensure the system is maintained and used consistent with the authorities of the Department, ICE HSI created a governance process to monitor the ongoing operations of FALCON-SA, to decide requests to add new data sources to the system, and to establish policies and procedures that govern system operation and user behavior. The governance process is staffed by HSI leadership and senior managers, and advisory services are provided by the Office of Principal Legal Advisor, the ICE Privacy Office, and the ICE Office of Chief Information Officer. This governance process helps ensure that new data sources are appropriately vetted for legal and privacy risks, as well as compliance with the DHS Fair Information Practice Principles. In addition, the routine ingestion of data from any new data source will require an update to the Appendix of this PIA and approval from the DHS Chief Privacy Officer. For *ad hoc* data uploads, the existence of supervisory oversight and review helps to ensure that new data will conform to ICE policy requirements that define what information is appropriate to include the system.

To address the risk that FALCON-SA users will have access to data unrelated to their official duties, ICE policy requires that FALCON-SA data-access restrictions be based on need to know and job responsibilities. FALCON-SA's underlying technology supports this requirement by providing the system owner and individual users with the ability to finely tune access to information on a data-point-by-data-point basis (i.e., at the sub-record level). For data routinely ingested into FALCON-SA from another source, the system permits access based on the users' original access privileges in the source system.[3] This prevents users from accessing data in FALCON-SA that they cannot access in the source system. For *ad hoc* uploads of data, the uploading user must affirmatively grant access to others either by granting view-only access to the data stored in the user's project, or by publishing the data. Adjustments to access permissions are reflected throughout the enterprise in a matter of minutes, and when permission to access data is withdrawn any user actively working with that data is logged out of the system. Additionally, the system is aware if any part of a shared or published search query or visualization contains information that a user is not authorized to access, and blocks that user's access to the entire search or visualization.

[3] In some circumstances, access to a routinely ingested data source may be provided via FALCON rather than by granting the user access to the source system. This determination is made by HSI on a case by case basis, after it has been determined that the user has a need-to-know and with the authorization of the data owner.

To mitigate the risk of authorized users conducting searches for inappropriate purposes, FALCON-SA implements extensive auditing of user actions in the system. User actions are recorded and stored in audit logs accessible only to supervisors and ICE IT security personnel, which are searched and analyzed to ensure proper usage of the system. Audit data is also available to ICE Office of Professional Responsibility (OPR) investigators if there is an investigation into possible wrongdoing by a FALCON-SA user.

To combat the risk of authorized users uploading data the system is not authorized to hold, ICE policy requires that users grant their supervisors access privileges to all projects and data in their FALCON-SA virtual domains. This permits supervisors to view how their staff members are using the system, including the specific data they are importing and working with and the types of investigations and/or analyses they are conducting. When *ad hoc* data is imported into FALCON-SA, supervisors are responsible for identifying and deleting any data imported in contravention of ICE policy. Users are also required to enter information describing the data being uploaded, such as source name/category and date retrieved, which helps the supervisor evaluate whether the upload complies with ICE policy and helps other users better understand and evaluate the data. Finally, FALCON-SA audits all *ad hoc* uploads by recording user name and date/time of upload.

The publication of visualizations and *ad hoc* data to the system is also controlled by supervisors to ensure an appropriate level of dissemination, and all publication activities are fully audited by the system. If the user leaves the unit or HSI, the supervisor will control access privileges to the user's visualizations. Users must also receive supervisory approval prior to extracting visualizations from FALCON-SA. FALCON-SA also records all extracts by recording the user name, date, and time of the extracted visualization, as well as which visualization was extracted. The extracted visualization does not include the source records, but parts of the records that created the particular visualization.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

ICE is authorized to collect this information pursuant to 8 U.S.C. § 1103 and § 1105; 8 U.S.C. § 1225(d)(3); 8 U.S.C. § 1324(b)(3); 8 U.S.C. § 1357(a); 8 U.S.C. § 1360(b); 19 U.S.C. § 1; and 19 U.S.C. § 1509. These authorities authorize ICE to collect and maintain information relevant to its immigration and customs investigations and other law enforcement responsibilities.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The DHS/ICE-006 ICE Intelligence Records System (IIRS) System of Records Notice (March 1, 2010, 75 Fed. Reg. 9233) applies to the information maintained in FALCON-SA.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

A System Security Plan (SSP) has been completed for FALCON-SA. The Security Authorization (SA) is currently scheduled to be granted on or about January 25, 2012.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

No. ICE is in the process of drafting a records retention schedule for NARA review. It will propose the retention periods for FALCON-SA records as described in Section 5 below.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

This system does not conduct information collections from the public and therefore it is not subject to the requirements of the Paperwork Reduction Act.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the project collects, uses, disseminates, or maintains.

Source Data

FALCON-SA assists the human evaluation and decision-making process and helps reduce human error and analytic uncertainty by presenting information already available to the user in a common sense fashion. FALCON-SA accomplishes this by storing and organizing data that is ingested into the FALCON-SA database on a routine or *ad hoc* basis from other existing sources, described in the Appendix to this PIA.

FALCON-SA contains information on individuals who have had previous encounters with DHS of a law enforcement nature, such as during a DHS investigation or during the inspection process at a port of entry. As FALCON-SA evolves, the population of individuals on whom data is maintained will change and this PIA will be updated accordingly. The addition of future datasets and populations of individuals is overseen by an internal ICE governance process (described in more detail below), which will consider the legal and privacy issues raised by the inclusion of other populations into this system given its purpose and ICE's legal authorities. The specific PII elements in FALCON-SA concerning any particular individual vary depending on what data the source records contain. Generally, FALCON-SA records may include some or all of the following types of PII: name, photograph, aliases, date of birth, citizenship and immigration status, nationality, immigration benefits, immigration history, admission information, customs import-export history, criminal arrest and conviction records, Alien Registration Number (A-Number), investigative case numbers, phone numbers, email addresses, residential and work addresses, identification document numbers, Social Security numbers, criminal associations, family relationships, employment, military service, education and other background information.

Index

FALCON-SA indexes and stores a table of the source data (routine and *ad hoc*) to make data searches more efficient. The index numerically and alphabetically lists every word or string of numbers/characters in the FALCON-SA database with a reference to the electronic location of the source record in FALCON-SA where that information is stored. The index may include any PII elements that are present in the source records, however, the index does not link together the PII elements for a single person. The index transforms data that may be difficult to search in the source systems because it is in a free form field into data that ICE users can find quickly and easily.

Metadata

FALCON-SA also captures metadata (i.e., data about data) about the various documents and other data ingested into the database on a routine basis or requires the user to create metadata on data ingested on an *ad hoc* basis. Metadata includes, but is not limited to, the name/title of the document, the specific source of the document or data, and the import date. If ad hoc data, metadata also consists of the user responsible for the import, the source name, the source category of the data imported (e.g., commercial data, finished intelligence reports, etc.), the date retrieved from the source, and associated ICE case number(s) (if any). PII may be contained in the file name of the imported data as well as in the identification of the ICE user responsible for the import.

Visualizations and Queries

The system uses visualization tools to present information in the database to the user in analytically useful ways. For example, the system can organize the information temporally or geographically or it can present a chart showing relational links between individuals and/or organizations. These visualizations reflect the content of the underlying source data and allow the user to identify links or connections that may have been previously unknown or to quickly search data that previously was difficult to access because, for example, in the source system it was in a free form text field but in FALCON-SA it is in a searchable index. The visualizations are only maintained so long as the data in the ingested source system remains. If the source system deletes a record, the record will no longer be available to the user for a particular visualization.. Using these visualization tools, FALCON-SA users work with data in their own virtual domains within FALCON-SA.

In circumstances defined by ICE policy, FALCON-SA users may also extract the visualizations from FALCON-SA and place them in another application, such as PowerPoint, for authorized use outside the system. Extractions can only be done with supervisory approval. When a visualization is extracted, the underlying source records are not extracted. Data may be extracted when necessary during the course of an investigation for visualizations, such as reports or presentations, for case management to include in case files, and for information sharing purposes.[4] The visualizations are used to illustrate how individuals, entities, groups, incidents or activities relevant to the investigation or analysis are connected.

Users may also create and save complex search queries within the FALCON-SA system. This prevents the user from having to re-enter search queries each time they logon to FALCON-SA. This is particularly useful for longer-term analytical projects and investigations, when the results of the query are expected to be valuable for ongoing analysis or incorporation into visualizations.

[4] FALCON visualizations that contain data supplied by non-DHS agencies are not shared outside of DHS unless such sharing complies with the Third Agency Rule or is authorized under the terms of information sharing agreements with the data owner. *See* Question 6.3.

2.2 What are the sources of the information and how is the information collected for the project?

FALCON-SA does not collect information directly from individuals, but rather accesses information collected, generated, and stored by and in other systems or from other information sources. FALCON-SA maintains a database containing information ingested on a routine or *ad hoc* basis from government databases, commercial data providers, and other sources. These data sources and the collection methods are listed in the Appendix to this PIA.[5]

Routine ingests of data from the sources listed in Section I of the Appendix occur by means of an automated "resyncing" process. FALCON-SA software periodically scans the source database to detect additions, modifications, or deletions to the records contained in the source system. The FALCON-SA database is then updated to reflect these changes.

Ad hoc ingests of data from the sources categories listed the Appendix occur either by users entering data manually or importing electronic files into the system via a data import application. The source of *ad hoc* ingests varies depending on the circumstances, but may include a particular user's knowledge, manual queries of other databases, reference materials, news reports, or other open source data. When importing electronic files to perform an *ad hoc* ingest, FALCON-SA requires the users to identify the category of the data source as defined in Section II of the Appendix.

The FALCON-SA system generates the index and visualizations described in Question 2.1 using the source data.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

Commercially available data and public (i.e., open source) data may be entered into FALCON-SA on an *ad hoc* basis by FALCON-SA users, but the system does not query or ingest data from these sources directly. FALCON-SA users have access to commercial or public sources outside the FALCON-SA system as part of their official duties, regardless of the existence and operation of FALCON-SA. Users may manually upload relevant records into FALCON-SA if they are deemed relevant to an investigation or ongoing project.

FALCON-SA users may use the commercial or public data as a way to verify or update information already in the system from other sources (e.g., a current residential address), or to add other information about an individual that not available in FALCON-SA, such as identifying data (e.g., date of birth), geospatial data, or public record data (e.g., civil litigations, criminal history, incorporation records). This data is used to cross-check, confirm, and broaden the scope of information available within DHS and users understanding of a particular matter. The geospatial data is also used to support visualization of the data on maps.

When users upload commercial or public data to FALCON-SA, they are required by ICE policy to input the following information into FALCON-SA: source category (either commercial or public); source name; the date retrieved; and the ICE case number for the investigation or analysis with which the uploaded data is associated. Users must also obtain supervisory approval for the upload. This

[5] As new datasets are added to this system, the Appendix to this PIA will be updated.

information is then linked to the uploaded data, along with metadata identifying the time of upload and the name of the user. This metadata is then visible to the other FALCON-SA users if and when the uploaded data is published to other users. Users who do not enter the information required by policy are identified and held accountable for any non-compliance during the supervisory review as well as through FALCON-SA audit logs.

2.4 Discuss how accuracy of the data is ensured.

FALCON-SA only assists the human evaluation and decision making processes associated with data retrieved from other systems; it does not collect information from the public or any other primary data source. Therefore, FALCON-SA relies on the system(s) and/or program(s) performing the original collection to provide accurate data. FALCON-SA users refer to a variety of data sources available through FALCON-SA and other systems to verify and correlate the available information to the greatest extent possible. Where incorrect information is identified, it is corrected either in FALCON-SA itself or in the source system, which then pushes the corrected data to FALCON-SA.

The accuracy of DHS-owned data, other government agency data, and commercial and public source data is dependent on the original source. Because of the law enforcement context in which FALCON-SA is used, there are often significant impediments to directly verifying the accuracy of information with the individual to whom the specific information pertains. For example, prior to an arrest, the agency may not have any communication with the subject because of the risk of alerting the subject that to the agency's investigation, which could result in the subject fleeing or altering his or her behavior in ways that impede the investigation. Since users have separate access to FALCON-SA source databases, as well as other databases and data sources, FALCON-SA users can actually assist in identifying and correcting inaccurate information by providing a basis for users to compare existing information and determine its context. FALCON-SA users are required by policy to make changes to the data in the underlying DHS system if they identify inaccurate data in FALCON-SA, or to otherwise notify the government data owner of inaccurate data.

For data sources routinely ingested into FALCON-SA (described in Section I of the Appendix), data is generally updated no less than every 48 hours to ensure that it is as complete and accurate as possible. The FALCON-SA index is updated on a daily basis. As the source system data is corrected, the data in FALCON-SA will be automatically updated and corrected as well. This automated data update process helps to ensure the data in FALCON-SA is as current and accurate as possible.

For *ad hoc* data uploads (described in Section II of the Appendix), in the event uploaded data is later identified as inaccurate, FALCON-SA users are required to modify their own *ad hoc* uploads to correct the data. If the user who uploaded the data no longer has access privileges to FALCON-SA, it is the responsibility of a supervisor or systems administrator to make the appropriate changes to the incorrect data. FALCON-SA users are trained how to modify *ad hoc* data for accuracy and correctness in the FALCON-SA system. In addition, data quality is strengthened by the policy requirement that all FALCON-SA users attach a case number to the uploaded *ad hoc* data, where one is available. Attaching a case number links the data to a particular investigation or analysis project, thereby helping to ensure the inclusion of the data in FALCON-SA is appropriate for investigative or analytical purposes. In addition, any *ad hoc* upload to the FALCON-SA system is reviewed and approved by a supervisor to ensure it is appropriate and in compliance with ICE policy.[6]

[6] *See* Question 8.1 below for discussion of the *ad hoc* upload review process and other controls to ensure proper use of the system.

FALCON-SA users are able to review source documents for specific data points in the system, allowing them to evaluate the origin of the records and data. Users also have access to complete data histories that reflect additions and edits to the data, allowing them to identify when and by whom modifications were made. During the analytical process, users also use metadata in the system to identify the source of data, when the data was uploaded (and therefore how current it is), and in the case of published visualizations by another FALCON-SA user, what links other users made, who the users are, and why the links were made. Users can validate the information in FALCON-SA with the source to ensure it is accurate, complete, and current, and thereby develop more accurate and useful analytical products. Because the data in the system identifies the ICE personnel responsible for entering *ad hoc* data, other users with access to that data can review and challenge its accuracy with that individual where appropriate.

FALCON-SA users receive training on the importance of verifying information from FALCON-SA before including it in any analytical report or using it as the basis for any formal law enforcement action, such as opening an investigation on an individual or arresting an individual for a crime.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

In addition to the risks accumulated by the underlying systems which FALCON-SA accesses or obtains data from (see Appendix), the following risks related to FALCON-SA's collection of data have been identified:

Privacy Risk: Because FALCON-SA permits users to upload information on an *ad hoc* basis, it is possible for a user to, accidentally or purposefully, input incorrect or biased information in the system.

Mitigation: FALCON-SA automatically captures the identity of the user who uploads the information, resulting in full attribution to the user who provided it. By policy, ICE requires users to input the source name and category and the date of data retrieval, which helps other users assess data quality. Users are authorized to upload records and information which are pertinent to the particular project in FALCON-SA they are working, e.g., an investigation or an analysis project. Users are not permitted to upload extraneous materials or records that are not related to their official duties and assignments. FALCON-SA also requires supervisors to review and approve *ad hoc* uploads, thereby ensuring the data is reviewed for flaws or non-compliance with ICE policy before it is used or made available in the system. If a user provides incorrect or biased information, the information can be corrected and remedial or disciplinary action taken against the user, if appropriate.

Privacy Risk: Because FALCON-SA is a data aggregation and analysis system, it is possible that information will be included in the system that is not necessary and relevant to accomplish the system's purpose.

Mitigation: ICE established safeguards to prevent the inclusion of data that does not serve FALCON-SA's intended purpose to support ICE HSI law enforcement investigations and analytical activities. HSI created a governance process to monitor the ongoing operations of FALCON-SA, to decide requests to add new data sources to the system, and to establish policies and procedures that govern system operation and user behavior. The governance process is staffed by HSI leadership and senior managers, and advisory services are provided by the Office of Principal Legal Advisor and the ICE Privacy Office. The existence of this governance process will help to ensure that new data sources are appropriately vetted for legal and privacy risks, as well as compliance with the DHS Fair Information

Practice Principles. In addition, the routine ingestion of data from any new data source will require an update to the Appendix of this PIA and approval from the DHS Chief Privacy Officer. For *ad hoc* data uploads, the existence of supervisory oversight and review helps to ensure that new data will conform to ICE policy requirements that define what information is appropriate to include the system.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

FALCON-SA assists the human evaluation and decision making process and helps reduce human error and analytic uncertainty by presenting information already available to the user in a common sense fashion. FALCON-SA is used by ICE HSI agents, criminal research specialists, and analysts to enforce and investigate violations of U.S. criminal and administrative laws administered or enforced by ICE, and to produce law enforcement intelligence supporting the same. FALCON-SA also allows ICE to increase the efficiency of multiple data source searches and identification of similar, identical, or related information from existing but disparate datasets. FALCON-SA-assisted research is used to produce law enforcement intelligence products, provide lead information for investigative inquiry and follow-up, to assist in the disruption of terrorist or other criminal activity, and to discover previously unknown connections among existing ICE investigations.

FALCON-SA assists ICE personnel in the analytical process that ultimately leads to the generation of law enforcement intelligence products, which are analytical reports that better inform ICE leadership and law enforcement personnel about criminal tactics, trends, and other developments. These analytical products help inform a variety of agency goals, decisions or strategies, such as how ICE resources are distributed among geographic areas, what the agency's operational priorities are, and what countermeasures or tactics are likely to be effective in disrupting specific types of criminal activity. ICE personnel use FALCON-SA to obtain a more comprehensive view of available data, and then analyze and interpret it using FALCON-SA's visualization and collaboration tools.

FALCON-SA source data is used to identify individuals, associations, relationships, or trends that relate to ICE's authorities and mission and may assist ICE in identifying or preventing criminal activity. Search queries are performed against the system's index. Index data facilitates efficient searching of large datasets for terms that occur in structured or free-text data fields. By allowing users to perform a single query across multiple datasets, FALCON-SA reduces the time users would have spent searching each individual system and reduces the load placed on those systems through repeated queries. User-provided information and other *ad hoc* uploads of data are used to complement or clarify data already in FALCON-SA. The mapping/imagery data allows users to view information in a geographic context.

FALCON-SA's metadata provides users with information about a particular record or piece of data, such as its source, date and time of ingest, the user who uploaded it (for *ad hoc* uploads), case numbers, and the name of the record. This system uses the metadata to apply rules that govern the record or data, such as access control lists that determine which users are permitted to search, view, and analyze it. The metadata also help FALCON-SA users to gain a more complete understanding of the data. For example, a user may use the identity of the data source as a way to assess the likely reliability of the information, or view the date the record was uploaded and know that more recent information is likely available in another system. The metadata also allows users to validate the information in FALCON-SA with the source to ensure it is accurate, complete, and current.

FALCON-SA also enhances how ICE uses data it already collects by permitting visualization of the data. FALCON-SA's visualization tools help users discover connections among individuals, groups, incidents, or activities. The tools also allow users to organize and view the data in a variety of ways. The visualization tools include:

- Link charts representing relationships between different entities (people, addresses, organizations, etc.);
- Various graphical depictions of the chronology in which events occurred; and
- Geospatial placement of entities or events on a map.

These tools assist the user in conducting analysis to assist with investigations or to create analytical products. HSI users will use these tools to identify trends, develop investigative leads, discover connections among investigations and targets, and enhance the overall investigative and analytic process. Users may extract visualizations from the system for a variety of law enforcement purposes, for example, to use as attachments to analytical products or presentations, or as reference materials for investigative teams and task forces. The users maintain the visualizations they create within their own virtual domain in FALCON-SA, but they may elect to publish the visualization in the system, which then shares it with all or a select list of FALCON-SA users. Publication of visualizations must be approved by a supervisor in advance.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

In response to user-specified queries, FALCON-SA uses technology to assist its users in recognizing relationships among persons, resolving commonalities, and identifying differences in existing information holdings. This helps the user to better understand individual and organizational relationships. FALCON-SA presents information in the database to the user in analytically useful ways. For example, the system can organize the information temporally or geographically or it can present a chart showing relational links between individuals and/or organizations. These visualizations reflect the content of the underlying data and serve to assist the human evaluation and decision making process. They help reduce human error and analytic uncertainty by presenting information already available to the user in a common sense fashion.

FALCON-SA's tools assist users in recognizing relationships, using data (e.g., names, identifying numbers, addresses) to resolve entities with similar properties into a single identity, understanding organizational relationships, and developing timely, actionable leads needed to accomplish law enforcement and law enforcement intelligence objectives, and the administration of immigration laws and other laws administered or enforced by ICE. When a user resolves an entity, i.e., determines that information from two sources pertains to the same individual, FALCON-SA retains a history of both resolved entities. This history permits a user to undo the resolution of the entity at a later time if it is discovered that the entity resolution was done in error. All FALCON-SA users have access to the information in the entity resolution history and can view the process by which another user determined that two or more entities were a single entity.

FALCON-SA users can create and share persistent searches that regularly search the database for new information matching the user-defined search criteria. FALCON-SA users can also create and share

complex search queries that have been shown to return useful results. Users can also export data in various formats that can be saved by the user on their workstation. Any such exports are approved by supervisors, then recorded and retained in the FALCON-SA audit logs.

3.3 Are there other components with assigned roles and responsibilities within the system?

No. At this time, the only individuals authorized to access FALCON-SA are ICE personnel and supporting contractors, other federal personnel assigned to ICE, and other federal personnel who are assigned to an ICE task force.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: Because FALCON-SA aggregates data from multiple data systems, it is possible that its users may be able access records in FALCON-SA that they otherwise could not view in the source system and are inappropriate for them to access.

Mitigation: For data sets routinely ingested into FALCON-SA, ICE has established technical rules to ensure that the user privileges of the source system carry forward and apply to that user in FALCON-SA. As a result, a user's access privileges to the data stored in FALCON-SA are identical to their access privileges to that same data in the source system. This prevents FALCON-SA from being used, intentionally or unintentionally, to undermine or defeat the role-based access controls established by the source system.

In some cases, however, ICE may use FALCON-SA to facilitate new access to a particular dataset in FALCON-SA by certain individual users or user groups. These types of exceptions are only made on a case-by-case basis after a determination that the new users have a demonstrated need-to-know, and with the authorization of the data owner. These controls mitigate the risk that data will be shared with FALCON-SA users who lack a need-to-know.

Privacy Risk: There is a risk that FALCON-SA users will use the system tools and data for purposes beyond what is described in this PIA.

Mitigation: FALCON-SA has a robust auditing feature that helps to identify and support accountability for user misconduct. User activity is audited heavily, including actions such as uploading records or data, extracting information from the system, resolving entities, searches, and viewing records. ICE has established controls that are based in policy and where possible enforced by technology, that provides clear instruction on what the authorize uses of the system are. Disciplinary action for violations of ICE policies regarding the system is taken where warranted. Before they receive access to the system, all users are trained on system use and other policies governing the system. In addition, FALCON-SA's access controls are highly customizable and can be set at the record or even data field level. This ensures that users without a need to know are technically barred from accessing that information. Question 8.1 contains an in-depth discussion of all controls that help to ensure the system and its information are used in accordance with the practices stated in this PIA.

Privacy Risk: There is a risk that information that was not readily accessible prior to the index will now be accessible and link individuals inappropriately.

Mitigation: Users are trained to review the linkages and to determine whether the linkage is appropriate.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

FALCON-SA does not directly collect information from individuals. FALCON-SA simply allows authorized ICE agents, investigators, officers and analysts to increase the efficiency of multiple data source searches and to identify similar, identical, or related information from existing but disparate datasets the user already has access to. General notice of the existence, contents and uses of this system and the systems that it routinely derives its data from are provided by the publication of this PIA and the associated SORNs. Because FALCON-SA is a data aggregation system that operates for law enforcement purposes, it is not feasible or advisable to provide notice to all individuals at the time their information is collected or input into FALCON-SA. With respect to information obtained from individuals through federal government forms or other means, such as information collected pursuant to seizures of property, notices on any such forms state that their information may be shared with law enforcement entities. As part of this PIA process, DHS reviewed the applicable SORNs to ensure that the uses were appropriate given the notice provided.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Because FALCON-SA does not directly collect information from individuals, opportunities for the individual to consent, decline, or opt out are limited or non-existent. The agency or program that actually collected the information from the individual is best positioned to provide them with the opportunity to consent, decline to provide information, or opt out.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: Because FALCON-SA does not collect information from individuals directly, individuals are unlikely to know at the time of collection that their data will reside in FALCON-SA. There is a risk that these individuals are unaware of the system and the purposes for which their data will be used.

Mitigation: The publication of this PIA helps to mitigate the lack of direct notice to the individual whose information is placed into FALCON-SA. This PIA provides a description of the types of records that will be placed into FALCON-SA on a routine or *ad hoc* basis, the purposes for which the information will be used by ICE and the tools that will be used to analyze the data. In addition, individuals who suspect information about them is stored in FALCON-SA may seek to access the information by following the procedures described in Section 7, Redress. Although not all information

may be available upon request due to law enforcement sensitivities, ICE will provide access to the extent that it does not interfere with an ongoing investigation or analysis, or reveal investigative techniques and sources.

Privacy Risk: Because individuals are not provided with notice, an opportunity to consent, opt-out, or decline to have their information included in FALCON-SA, there is a risk that inappropriate data will be placed in FALCON-SA.

Mitigation: ICE established safeguards to prevent the inclusion of data that does not serve FALCON-SA's intended purpose of supporting ICE HSI law enforcement investigations and analytical activities. HSI created a governance board to monitor the ongoing operations of FALCON-SA, to decide requests to add new data sources to the system, and to establish policies and procedures that govern system operation and user behavior. The governance board is staffed by HSI leadership and senior managers, and advisory services are provided by the Office of Principal Legal Advisor and the ICE Privacy Office. The existence of this governance process will help to ensure that new data sources are appropriately vetted for legal and privacy risks, as well as compliance with the DHS Fair Information Practice Principles. In addition, the routine ingestion of data from any new data source will require an update to the Appendix of this PIA and approval from the DHS Chief Privacy Officer. For *ad hoc* data uploads, the existence of supervisory oversight and review helps to ensure that new data will conform to ICE policy requirements that define what information is appropriate for uploading into the system.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

The retention period for the 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 and SORN of the source system. Once an underlying source system deletes or changes the data, FALCON-SA will delete or change its data during its next refresh from that system. Any records input into FALCON-SA (emailed zip files, CD-ROMs, etc.) will be destroyed after upload and verification to FALCON-SA, or returned to the source.

FALCON-SA data uploaded in an *ad hoc* manner are retained in the system for the same length of time as the associated ICE case file (if an associated ICE case exists, ICE policy requires the user to enter the ICE case number when uploading into FALCON-SA or at any appropriate time thereafter). If there is not an ICE case number associated with the uploaded data, the retention period is twenty (20) years.

FALCON-SA metadata and index data are retained for the same length of time as the record or data element they describe or originate from. FALCON-SA accounting for disclosure forms are retained for five (5) years and then purged. FALCON-SA's user-created visualizations and search queries that have an associated ICE case number are maintained for the same retention period as applies to that case. If no case number is assigned, visualizations and search queries are maintained in the user's virtual domain for twenty (20) years or until the user deletes them, assigns a case number (which will then apply that case's retention period), or the user's account is terminated, whichever comes first. Visualizations

and search queries containing PII but without an associated case number must be recertified annually by the user or supervisor, or the information is purged from the system.

Once a FALCON-SA source record or item of data is deleted from the system because the retention period has expired, that data will also be deleted from the metadata, index, and any user-created visualizations and search queries.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that information in FALCON-SA will be retained for longer than necessary and appropriate given the purpose of the system and the original reason the information was collected.

Mitigation: In the case of routinely ingested data, FALCON-SA retains the information for the same length of time as the source DHS system. This ensures data is not retained longer than necessary or in a way that is inconsistent with the original purpose of collection, as the original program or agency was in the best position to determine the appropriate length of retention given the purpose. For *ad hoc* uploads of data, if the user associates it with an ICE case by adding a case number, the retention period for that case will be applied. This ensures that these records are treated in the same manner as other case-related records, and is consistent with the law enforcement investigative or analytical purpose for which the record was uploaded. Any *ad hoc* uploads that are not associated with a case are retained for a default period of twenty (20) years, unless otherwise specified in Appendix A. In any case, *ad hoc* data obtained from other federal systems of records will not be retained longer than the original retention period unless that data is associated in FALCON-SA with an ICE case number.

Visualizations and search queries are also retained for the associated case retention period, if a case number is assigned; otherwise, they are retained for a maximum of thirty (30) years provided any with PII are recertified at least annually. This policy ensures that user-created visualizations and searches are only retained as long as needed for a related ICE case, or that the user or supervisor has specifically certified an ongoing law enforcement need for retention.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government, and private sector entities.

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Access to FALCON-SA is limited to ICE users only (including contractors, task force members, and persons assigned to ICE from other agencies). ICE routinely shares ICE-generated intelligence reports and investigative information with law enforcement or intelligence agencies that demonstrate a need to know the information in the performance of their missions. These reports and investigative data may contain visualizations created within and extracted from the FALCON-SA system. This sharing occurs if it will further HSI's own law enforcement analyses or investigations, and provided that disclosure is consistent with applicable law and the IIRS SORN. These agencies can include federal,

state, tribal, local and foreign law enforcement agencies, as well as relevant fusion centers, FBI Joint Terrorism Task Forces, and international organizations such as INTERPOL.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

The sharing of PII with law enforcement or intelligence agencies outside of the Department is compatible with the law enforcement purposes of the original collections listed in the SORNs of the underlying data sources, as well as the law enforcement intelligence purpose described in the IIRS SORN.

6.3 Does the project place limitations on re-dissemination?

Users of FALCON-SA will use the processes and procedures already established within DHS and ICE about the sharing of data internally within DHS and external to the Department. Users will observe the third agency rule, which encourages that prior to sharing another agency's data with a third agency (not involved in the original sharing agreement) the agency that intends to share will acquire consent from the agency that provided the data. However, by agreement with certain agencies that provide data to ICE, ICE received advance authorization to share their information with specified third parties and/or for specified purposes.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

By policy and via user training, users are instructed to record any disclosure of information from FALCON-SA outside of DHS by completing an accounting for disclosure form in FALCON-SA. The form captures the date, nature, and purpose of the disclosure and the recipient's information.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that data will be shared with external parties lacking a need to know, and that external sharing will not be properly recorded as required by the Privacy Act.

Mitigation: FALCON-SA users are required by law and policy, which is reinforced by user training, to share information from FALCON-SA with only those external partners who have a law enforcement, intelligence, or national security need-to-know. This requirement is in keeping with the law enforcement purpose of the system and the scope of ICE's mission as a law enforcement agency. Users are required to complete an online form in the system when making an external disclosure to comply with the provisions of the Privacy Act, 5 U.S.C. § 552a(c).

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

7.1 What are the procedures that allow individuals to access their information?

Individuals seeking notification of and access to any record contained in FALCON-SA, or seeking to contest its content, may submit a request in writing to ICE FOIA Officer, by mail or facsimile:

U.S. Immigration and Customs Enforcement
Freedom of Information Act Office
500 12th Street SW, Stop 5009
Washington, D.C. 20536-5009
(202) 732-0660
http://www.ice.gov/foia/

All or some of the requested information may be exempt from access pursuant to the Privacy Act in order to prevent harm to law enforcement investigations or interests. Providing individual access to records contained in FALCON-SA could inform the subject of an actual or potential criminal, civil, or regulatory violation investigation or reveal investigative interest on the part of DHS or another agency. Access to the records could also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. *See* 75 Fed. Reg. 12437 (Mar. 16, 2010).

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

The correction procedures are identical to those described in Question 7.1 above. All or some of the requested information may be exempt from correction pursuant to the Privacy Act in order to prevent harm to law enforcement investigations or interests. Providing individual access to records contained in FALCON-SA could inform the subject of an actual or potential criminal, civil, or regulatory violation investigation or reveal investigative interest on the part of DHS or another agency. Access to the records could also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. *See* 75 Fed. Reg. 12437 (Mar. 16, 2010).

7.3 How does the project notify individuals about the procedures for correcting their information?

The information about correction is made available through the publication of this PIA and the associated SORNs. Because FALCON-SA contains copies of datasets owned by DHS components and offices or other agencies, individuals may also have the option to seek access to and correction of their data directly from those agencies or offices that originally collected it. Information that is corrected in the original source system will be updated in the FALCON-SA data repository during routine refreshes thereby ensuring accurate and current information.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals will be unable to meaningfully participate in the use of their data as maintained in this system, or determine whether the system maintains records about them.

Mitigation: Because the data in this system originates from other systems of records with a law enforcement purpose, individuals' rights to be notified of the existence of data about them, and to direct how that data may be used by ICE, are limited. Notification to affected individuals could compromise the existence of ongoing law enforcement activities and alert individuals to previously unknown investigations of criminal or otherwise illegal activity. This could cause individuals to alter their behavior in such a way that certain investigative tools, such as wiretaps or surveillance, will no longer be useful. Permitting individuals to direct the agency's use of their information will similarly interfere with the intended law enforcement use of the system.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

FALCON-SA uses various technological and policy-based controls described below to help ensure that FALCON-SA information is used in accordance with the stated practices in this PIA.

Robust Access Controls. ICE policy requires that FALCON-SA access restrictions be based on users' need to know and job responsibilities. FALCON-SA's underlying technology provides the system owner and individual users with the ability to finely tune access to information on a data-point-by-data-point basis (i.e., at the sub-record level). Access to each data point is controlled by access control lists created at the system and user level in FALCON-SA. For data routinely ingested into FALCON-SA from another source, the access control lists are based on the users' original access privileges in the source system.[7] This is accomplished by passing individual user credentials to the originating system or through a previously approved certification process in another system. This safeguard prevents a user from being able to access data in FALCON-SA that they are unable to access in the source system. For *ad hoc* uploads of data, the user that performed the upload must affirmatively grant access to others either by granting view-only access to the data within the uploading user's virtual domain or by publishing the data to the system.

Adjustments to access permissions are reflected throughout the enterprise in a matter of minutes, and when permission to access data is withdrawn any user actively working with that data will be logged out of the system. Additionally, the system prevents users from indirectly accessing records or data they are not authorized to view via another user's search query or visualization. If any part of a shared or published search query or visualization contains information that a user is not authorized to access, the system blocks that user's access to the query or visualization.

Robust and Accessible User Auditing. FALCON-SA also implements extensive auditing of user actions in the system. User actions are recorded and stored in audit logs accessible only to authorized personnel. The audit logs are protected from unauthorized access, modification, and destruction that would negate their value. User auditing captures the following activities: logon and logoff, search query strings, records viewed by the user, changes in access permissions, records/reports extracted from the system, and records/reports printed by the system. The system also keeps a complete record of all

[7] In some circumstances, access to a routinely ingested data source may be provided via FALCON rather than by granting the user access to the source system. This determination is made by HSI on a case by case basis, after it has been determined that the user has a need-to-know and with the authorization of the data owner.

additions, modifications, and deletions of information in the system, the date/time, and user who performed the action. This information is readily accessible by supervisors and ICE IT security personnel, and can be searched and analyzed to ensure proper usage of the system. This information is also available to ICE Office of Professional Responsibility (OPR) investigators if there is an investigation into possible wrongdoing by a FALCON-SA user.

General Supervisory Oversight and Monitoring. ICE policy requires that users grant their supervisors access rights to all work they are performing in their FALCON-SA virtual domains. This enables supervisors to view how their staff are using the system, including the specific data they are importing and working with and the types of investigations and/or analyses they are conducting. This policy helps to deter and identify users who are using the system or its data for unauthorized purposes, and to identify users who may be misusing the system due to inadequate training, so corrective action can be taken.

Tagging, Supervisory Monitoring, and System Auditing of Ad Hoc Data Uploads. When *ad hoc* data is imported into FALCON-SA, users are required by policy to electronically share this data with their supervisors for review. Supervisors are alerted when new data has been shared with them and are responsible for identifying any data imported in contravention of ICE policy. Supervisors may request that any such data be deleted from the system, with the approval of the HSI unit chief that serves as the system owner. Users are also required to enter information describing the data being uploaded, such as source name/category and date retrieved, which helps the supervisor evaluate whether the upload complies with ICE policy and helps other users better understand and evaluate the data. Finally, FALCON-SA audits all *ad hoc* uploads by recording user name and date/time of upload.

Supervisory Control and System Auditing of Publication of Data to the System. The publication of visualizations and *ad hoc* data to the system is controlled by supervisors, and fully audited by the system. Publication permits visualizations and *ad hoc* data to be made generally accessible to other FALCON-SA users for search and analysis purposes. Publication can be tailored to just a group of users or to the entire FALCON-SA user community. Before a user may publish anything to the system, a supervisor must first approve to ensure the data is appropriate for the proposed dissemination. If the user leaves the unit or HSI, the supervisor will control access privileges to the user's visualizations. The supervisor would have the authority to maintain the information, delete the data, or transfer the data to another user who has taken over the initial user's investigation or analysis. FALCON-SA also audits all publications of visualizations by recording user name and date/time of upload.

Supervisory Control and System Auditing of Extracts from the System. Users must receive supervisory approval prior to extracting visualizations from FALCON-SA. FALCON-SA also records all extracts by recording the user name, date, and time of the extracted visualization, as well as which visualization was extracted.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All users will complete FALCON-SA training to include rules of behavior, appropriate uses of system data, uploading and tagging records, disclosure and dissemination of records, and system security. Users must complete training in order to receive authorization to access FALCON-SA. All personnel who have access to the ICE Network are also required to take annual privacy and security training, which emphasizes the DHS Rules of Behavior and other legal and policy restrictions on user behavior.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

Only ICE personnel who require access to the functionality and data in FALCON-SA as a part of the performance of their official duties will be granted access. Initial requests for access to the system are routed from the user to a supervisor, who validates that the user has a job related need-to-know and determines what user role should be assigned. Supervisors submit access requests to designated points of contact (POCs) who will validate that the user meets all requirements for access to the system, such as the appropriate level of background check. Once this is verified, the POC notifies a system administrator to create the user account, and the associated job-related user role that should be assigned. For personnel assigned to ICE on a task force or from other agencies, the same process is followed. However, in addition, any applicable agreement governing the task force or assignment is reviewed to ensure compliance.

User roles determine what specific functions users are authorized to perform in FALCON-SA. The basic FALCON-SA user roles are General User, Supervisor, and System Administrator. The General User is the most basic role and will permit the individual to do all the search and analysis functions in FALCON-SA. All General Users are permitted to enter/upload data and records subject to the restrictions describe elsewhere in this PIA. Each General User has his or her own virtual domain in the system. ICE agents, analysts, and research specialists will be assigned General User roles in FALCON-SA.

The Supervisor role has the same basic privileges of General Users, plus additional privileges that allow them to monitor and in some cases approve the activities of General Users in the system. For example, within the system, ICE intends to create a workflow process in the future whereby a General User that wants to publish a visualization to the system can request authorization from the Supervisor, and the Supervisor will have privileges in the system to authorize such publication. Supervisors will also eventually be able to view and query General User audit data, which captures the logon, search, upload, and publication actions of General Users in the system. As the system develops further, ICE expects to develop additional privileges for the Supervisor role. Only ICE supervisors will be permitted to hold a Supervisor user role in FALCON-SA.

The System Administrator role is assigned to those users who administer the system, and grants privileges to create accounts, change passwords, and perform other system support functions, including hard deletion of data where approved by HSI management. System Administrators may revoke a user's access when no longer needed or permitted.

User privileges may be customized beyond the user role initially assigned at account creation. For example, a particular ICE agent working on an investigative task force may be given privileges to access uploaded records seized during a search, along with other members of the task force. Because of investigative sensitivities related to the ongoing case, the task force may decide not to make these records widely available to other FALCON-SA users. Privileges to access these records would be assigned on a user-by-user basis by the user that uploaded those records or a supervisor. Appendix A describes in further detail the specific data that different categories of users may access in FALCON-SA. The user can also control the ability of other users to access data within the user's virtual domain (e.g., unpublished visualizations, ad hoc uploads, and search queries).

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

ICE established a governance process to monitor the ongoing operations of FALCON-SA, to decide requests to add new data sources to the system, to expand FALCON-SA user privileges to other DHS components or other agencies, and to establish policies and procedures that govern system operation and user behavior. The governance process is staffed by HSI leadership and senior managers, and advisory services are provided by the Office of Principal Legal Advisor and the ICE Privacy Office. The existence of this governance process will help to ensure that any proposals for new data sharing arrangements are appropriately vetted for legal and privacy risks, as well as compliance with the DHS Fair Information Practice Principles. In addition, formal written agreements between ICE and other agencies to share data or provide access to FALCON-SA would be reviewed by the ICE Privacy Office and Office of Principal Legal Advisor as a matter of routine. Also, the routine ingestion of data from any new source will require an update to the Appendix of this PIA and approval from the DHS Chief Privacy Officer.

Responsible Officials

Lyn Rahilly, Privacy Officer
U.S. Immigration & Customs Enforcement
Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

APPENDIX

I. Data Routinely Ingested into FALCON-SA

FALCON-SA ingests and permits users to query and analyze certain data from the following Privacy Act Systems of Records:

1) DHS/ICE-006 ICE Intelligence Records System (IIRS) SORN and DHS/ICE-009 External Investigations SORN.[8] From these systems of records, FALCON-SA receives law enforcement, intelligence, crime, and incident reports, and reports of suspicious activities, threats, or other incidents generated by ICE and other agencies. The ingest occurs at least once every 48 hours. All FALCON-SA users have privileges to view, query, and analyze this data maintained in FALCON-SA.

2) DHS/ICE-008 Search, Arrest, and Seizure Records SORN and DHS/CBP-013 Seized Assets and Case Tracking System (SEACATS) SORN.[9] From these systems of records, FALCON-SA receives ICE and CBP fines, penalties and forfeitures case records, seizure incidents, seized goods records, property information, and subject record data. The ingest occurs at least once every 48 hours. All FALCON-SA users will be able to view, query, and analyze this data maintained in FALCON-SA.

3) DHS/CBP-006 TECS SORN and DHS/ICE-009 External Investigations SORN.[10] From these systems of records, FALCON-SA receives lookout records created by ICE and CBP which are used for border screening. FALCON-SA also receives records concerning current or previous law enforcement investigations into violations of U.S. customs and immigration laws, as well as other laws and regulations within ICE's jurisdiction, including investigations led by other domestic or foreign agencies where ICE is providing support and assistance. The ingest occurs at least once every 48 hours. All FALCON-SA users will be able to view, query, and analyze this information maintained in FALCON-SA.

4) DHS/ICE-011 Immigration and Enforcement Operational Records System (ENFORCE) SORN.[11] From this system of records, FALCON-SA receives records of law enforcement agency applications for continued presence parole for victims and witnesses of human trafficking. The ingest occurs at least once every 48 hours. Only FALCON-SA users who are assigned to the Human Smuggling

[8] DHS/ICE/PIA-023 Significant Event Notification (SEN) System, July 26, 2010: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ice_sen.pdf. The DHS/ICE-006 ICE Intelligence Records System (IIRS) SORN was last published March 1, 2010 (75 Fed. Reg. 9233) and the DHS/ICE-009 External Investigations SORN was last published January 5, 2010 (75 Fed. Reg. 404).

[9] The DHS/ICE-008 Search Arrest and Seizure Records SORN was last published December 9, 2008 (73 Fed. Reg. 74732) and the DHS/CBP-013 Seized Assets and Case Tracking System SORN was last published December 19, 2008 (73 Fed. Reg. 77764).

[10] DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing, December 23, 2010: http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-cbp-tecs.pdf. The DHS/CBP-011 TECS SORN was last published December 19, 2008 (73 Fed. Reg. 77778). The DHS/ICE-009 External Investigations SORN was last published January 5, 2010 (75 Fed. Reg. 404).

[11] The DHS/ICE-011 Immigration and Enforcement Operational Records System (ENFORCE) SORN was last published May 3, 3010 (75 Fed. Reg. 23274).

and Trafficking Center (HSTC)[12] or to the ICE HSI Law Enforcement Parolee Unit will be able to view, query, and analyze this data in FALCON-SA.

II. Data Ingested on an *Ad Hoc* Basis into FALCON-SA

FALCON-SA contains records or data obtained from various data sources that are manually entered or uploaded by authorized FALCON-SA users. The entry of these records and/or data into FALCON-SA occurs on an *ad hoc* basis and is governed by ICE policy. Users are required by policy to obtain supervisory approval before *ad hoc* data is made available in FALCON-SA. Users who upload ad hoc data into FALCON-SA have the ability to restrict access to the data and allow access to those FALCON-SA users to view, query, and analyze this data on a need-to-know basis.

When uploading *ad hoc* data into FALCON-SA, users are prompted to select the appropriate source category that describes the source of the data. *Ad hoc* data is retained for the retention period of the ICE case it is associated with in the system (via entry of an ICE case number). If there is no associated ICE case, retention is twenty (20) years, unless otherwise specified below.

The source categories of *ad hoc* data are:

1) *Commercially available data:* Public and proprietary records available on people and businesses in commercial (subscription-based access) databases (e.g., CLEAR and Dunn & Bradstreet).

2) *Open source data:* News articles and reporting on various topics (e.g., Associated Press and the Open Source Center).

3) *CBP cargo and border crossing data:* Inbound/outbound shipment records and border crossing information from CBP's Automated Targeting System (ATS). PNR data obtained from ATS may not be uploaded or entered into FALCON-SA. These records will be retained in FALCON-SA for no longer than 15 years from the calendar year in which the border crossing or shipment occurred.

4) *Criminal information:* Criminal history information and warrant or other lookout records from domestic and foreign law enforcement sources, including the FBI's National Crime Information Center (NCIC) and on-going investigative information and data provided by local, state and other federal law enforcement agencies.

5) *Intelligence reports:* Finished intelligence reports generated by ICE, DHS, and other law enforcement or intelligence agencies. These reports will only be uploaded with the authorization of the agency that generated the report.

[12] The HSTC was established under Section 7202 of the Intelligence Reform Act and Terrorism Prevention Act of 2004. The secretary of state, the secretary of homeland security, the attorney general and members of the national intelligence community jointly oversee the HSTC through a high-level interagency steering group. The HSTC was established to achieve greater integration and overall effectiveness in the U.S. government's efforts to combat human smuggling, trafficking in persons, and clandestine terrorist travel. The HSTC coordinates activities with foreign governments to ensure that efforts are addressed globally. The HSTC brings together federal agency subject matter experts from the policy, law enforcement, intelligence and diplomatic arenas to work together and leverage all participating agencies' knowledge, expertise and authorities to address the global threat of illicit travel. ICE manages the day-to-day activities of the HSTC and has personnel assigned to work at the HSTC.

6) *Foreign government information:* Information or reports supplied by foreign governments and multinational organizations such as EUROPOL and INTERPOL relating to criminal history; immigration records; passenger, vehicle, vessel entry and exit history; passport information; vehicle, vessel and licensing records; shipment records; telephone records; intelligence reports; investigative leads and requests; and wants, warrants and lookouts.

7) *Evidentiary information:* In the context of investigations only, records concerning evidence seized or otherwise lawfully obtained during the course of an HSI investigation. This may include business records, records from other agencies, public court records, transcripts of interviews or depositions, or copies of records returned in response to a subpoena or seized during a search.