Privacy Impact Assessment
for the

FALCON Tipline

DHS/ICE/PIA-033

November 2, 2012

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

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) has deployed a new information system called FALCON Tipline (FALCON-TL), which is a component system of the larger HSI FALCON environment. This workflow management system supports the creation and maintenance of tips received by the HSI Tipline Unit about suspicious activity or suspected illegal activity, and the referral of this information to HSI field offices for appropriate investigation or other follow up. The ACRIMe Tipline Module, the system that the HSI Tipline Unit currently uses to track tips, is being replaced by FALCON-TL. This Privacy Impact Assessment (PIA) is necessary because FALCON-TL will maintain personally identifiable information (PII) about the individuals who are reporting the tips and are the subject of the tips.

Overview

The HSI FALCON Environment

ICE HSI recently created a new IT environment called "FALCON" to support its law enforcement and criminal investigative mission. The FALCON environment is designed to permit ICE law enforcement and homeland security personnel to search and analyze data ingested from ICE applications and systems, with appropriate user access restrictions at the data element level and robust user auditing controls. In February 2012, HSI deployed the first module of FALCON with the launch of FALCON Search & Analysis (FALCON-SA). FALCON-SA augments ICE's ability to review and develop information about persons, organizations, events, and locations by ingesting and creating an index of data from other existing operational government data systems and enabling ICE law enforcement and homeland security personnel to search, analyze, and visualize the data to help identify relationships. FALCON-SA supports ICE's mission to enforce and investigate violations of U.S. criminal and administrative laws. For more information on FALCON-SA, please see the FALCON-SA PIA.[1] The Appendix in the FALCON-SA PIA is being updated to capture FALCON-TL as data routinely ingested into FALCON-SA. FALCON-TL and other FALCON modules will be deployed in support of discrete HSI mission areas and work units.

FALCON Tipline (FALCON-TL)

The HSI Tipline Unit is a 24-hour, seven days a week operations center. The Unit supports ICE's intake of and response to reports of suspicious activity or suspected illegal activity made by members of the public and other law enforcement agencies. Members of the public and most law enforcement agencies, including state and local police departments, submit tips via an online form on the ICE website or by calling the HSI Tipline at (866) 347-2423 ((802) 872-6199 for those calling outside the United States). Some law enforcement agencies, such as the Federal Bureau of Investigation (FBI), the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), and other components of the Department of Homeland Security (DHS), may also submit tips by directly e-mailing the HSI Tipline Unit. Tips

[1] See DHS/ICE/PIA-032 FALCON Search & Analysis System at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ice_falconsa.pdf.

received describe various suspected or actual illegal activities including drug smuggling, illegal exports, document and benefit fraud, alien fugitives, alien smuggling, bulk cash smuggling, child pornography/exploitation, and human rights violations. The HSI Tipline Unit records these tips and refers them to HSI field offices for investigation or other appropriate follow up. This PIA covers all tips received by the HSI Tipline Unit regardless of how they are received.

Currently, specialists working in the HSI Tipline Unit use the Tipline Module within the Alien Criminal Response Information Management System (ACRIMe) to record incoming tips. For more information on the ACRIMe Tipline Module, please see the ACRIMe PIA.[2] With the launch of FALCON-TL, ICE will migrate the data from the ACRIMe Tipline Module into FALCON-TL and retire the Tipline Module. HSI Tipline Unit personnel will input all new tips received into FALCON-TL.

As noted above, the HSI Tipline Unit receives tips by telephone, e-mail, and through the ICE public website.[3] If the tip is made by telephone, the HSI Tipline specialist speaks with the caller and enters information about the tip and the caller in FALCON-TL. It should be noted that prior to speaking with the HSI Tipline specialist, the caller hears a message. The message alerts the caller that the call is being recorded, that he or she can choose to remain anonymous when providing the tip, and that information provided may be forwarded to the appropriate ICE field office for investigation, as appropriate. The HSI Tipline specialist also enters information on tips submitted through the ICE public website or via email. Tip records created in FALCON-TL include the nature of the possible violation of law or suspicious activity being reported, any details provided such as the individual(s) or entities suspected to be or actually involved, the location, and metadata (i.e., data about data) associated with the processing of the information. Individuals submitting the tip (if they do not choose to remain anonymous) will be asked to provide their name and other identifying and contact information. FALCON-TL automatically generates a tracking number for each tip record created in the system.

After receiving the tip, the HSI Tipline specialist inputs the relevant data into FALCON-TL. There are two components of a FALCON-TL record – the report narrative component, which contains all the information related to the tip, and the report subject properties component, which contains a subset of the information in the report narrative component. When a Tipline specialist creates a tip, he or she completes the report narrative component and FALCON-TL creates the associated report subject properties component. The Tipline specialist then conducts a search in FALCON-SA and other government, open source, and commercial databases to identify additional information related to the tip. For example, if an incoming tip provides very specific identifying information about the person alleged to have violated a law that is enforced by ICE, the Tipline specialist's research in FALCON-SA may reveal that the individual is already the subject of an open ICE investigation. Tipline specialists may also use the various visualization tools described in the FALCON-SA PIA, and attach relevant visualizations to the tip record in FALCON-TL. Information that may be added to a tip includes geospatial data, information from news reports, and information from public records including civil litigations, criminal history information, and state incorporation records. When creating a tip in FALCON-TL, a Tipline specialist also searches existing tips in FALCON-TL to see if the tip is a duplicate of one already in the

[2] *See* the DHS/ICE/PIA-020 - Alien Criminal Response Information Management System (ACRIMe), April 22, 2010, and the subsequent PIA updates (http://www.dhs.gov/files/publications/gc_1279833335485.shtm#19).
[3] http://www.ice.gov/exec/forms/hsi-tips/tips.asp.

system.[4] Users manually search for key words and other information to help locate duplicate tips. If the tip is a duplicate, the specialist consolidates the tip records into one FALCON-TL record.

After the tip record is created, the Tipline specialist forwards it to a supervisor for review within the system. The supervisor reviews the tip to determine if it is "actionable," which means it is appropriate for the supervisor to forward the tip within FALCON-TL to a point of contact (POC) in the appropriate HSI field office for further investigation. Once forwarded, the tip moves into FALCON-SA and is now accessible by all FALCON-SA users. For certain "actionable" tips, the supervisor may also direct that a subject record be created in TECS (via a separate manual process) to serve as a lookout record for the individual, vehicle, or other subject that is of law enforcement interest.[5] If the supervisor determines the tip is not "actionable," no further work is done and the tip record is ingested into FALCON-SA, where it is available to the broader group of HSI personnel who use the FALCON-SA system to do research and analysis. Once a FALCON-TL record has been moved to FALCON-SA, FALCON-SA users can only modify the information in the report subject properties component. If a FALCON-SA user is using a tip record as part of the research he or she is doing and discovers an error in the record (for example, the phone number listed is wrong), the FALCON-SA user can update it in the report subject properties component without changing any information in the report narrative component. A FALCON-TL user would need to make the corresponding change in the report narrative component. Enabling FALCON-SA users to only modify the report subject properties component of a tip record helps to improve data accuracy in the system.

Periodically, ICE receives tips regarding illegal activity that does not fall within ICE's jurisdiction but is the responsibility of another agency to investigate. These tips are entered in FALCON-TL and marked as "actionable" by the supervisor. The HSI Tipline Unit then either refers the tip to the investigating agency for action, or forwards the tip to the appropriate HSI field office, to handle the referral.

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

[4] As part of the initial FALCON-TL installation, all records from the ACRIMe Tipline Module will be imported into FALCON-TL, where they will be searchable and retrievable by all FALCON-SA users.
[5] For more information on the purpose and use of TECS subject records, see the DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing at http://www.dhs.gov/privacy-documents-us-customs-and-border-protection#8, and the DHS/CBP-011 TECS SORN (73 FR 77778) at http://www.gpo.gov/fdsys/pkg/FR-2008-12-19/html/E8-29807.htm.

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

The DHS/ICE-007 - Law Enforcement Support Center (LESC) Alien Information Management (ACRIMe) SORN[6] applies to the information maintained in FALCON-TL. This SORN is currently being updated to, among other things, change the name of the system of records to the Alien Criminal Response Information Management System (ACRIMe) System of Records.

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. The Security Authorization (SA) was granted on January 30, 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 period for FALCON-TL 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.

The tip form on the ICE website collects information from the public and is subject to the requirements of the Paperwork Reduction Act. The form's OMB control number is 1653-0049 and the expiration date for OMB's approval is September 30, 2014.

Section 2.0 Characterization of the Information

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

Below are the various types of information FALCON-TL collects, uses, maintains, or disseminates. Not all information listed may be collected on any given tip.

Tip Information

- Allegations: Type of suspicious or illegal activity or event, circumstances around the activity, location information about the activity (address, city, state, zip code), and date and time of the

[6] See DHS/ICE-007 LESC ACRIMe SORN at http://www.dhs.gov/system-records-notices-sorns#6.

activity. Also, any documents or other files submitted with the tip, such as tip emails sent to the HSI Tipline Unit and any files sent as attachments to the tip.

- Associated Individuals or Entities: Any information about the individuals or entities alleged to be involved with the suspicious or illegal activity or event, such as:
  - Identifying information, such as name, address, phone number, date of birth, Alien Registration Number, and Social Security Number.
  - Citizenship and immigration history information, criminal history information, incorporation records, litigation information.
  - Any other information submitted by the person providing the tip or the referring agency.
  - Any other information found by the HSI Tipline Unit during research in FALCON-SA, other DHS or government databases, or public source and commercial data research.
- Information About the Tip Provider: Information about the individual (whether a member of the public or an employee of a law enforcement or other government agency) submitting the tip, such as name, agency, address, phone number, fax number, and e-mail address.
- ICE field office or the outside agency to which the tip was referred and any relevant follow-up information related to the tip including a case number.
- The tip record's unique system-generated identifier in FALCON-TL.

Metadata

FALCON-TL captures metadata about the records created in the system. Metadata on records includes, but is not limited to, the name of the HSI Tipline specialist inputting the tip and the time and date the information was entered. PII may be contained in the identification of the ICE user responsible for the entry. In addition to the metadata mentioned above, the e-mail address of the person sending the tip and the date and time of the e-mail are captured for tips that are submitted via e-mail.

In addition to the metadata mentioned above for records created in the system, the following metadata is captured on the tips submitted through the tip form on the ICE public website:

- Internet domain, i.e., "xcompany.com" if the person is using a private Internet access account or "xyzschool.edu" if the person is connecting from a university's domain
- Internet protocol (IP) address
- Browser software and operating system
- Date and time of the ICE website visit
- Internet address of the website from which the person linked to the ICE website

Reports

FALCON-TL and FALCON-SA users will be able to use the reporting capabilities in the system to generate reports for internal ICE uses. Reports are generally statistical in nature and show information such as the number of tips received in a given week or the number of tips received for a particular investigative case category such as alien smuggling, bulk cash smuggling, or human rights violations. Some reports may contain PII and be used to manage the investigation and resolution of tips received by the HSI Tipline Unit and subsequent referrals to HSI field offices.

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

The HSI Tipline Unit receives a majority of tips by telephone. The HSI Tipline Unit also receives tips via the tip form on the ICE public website and via e-mail from other law enforcement agencies. After a tip has been received, an HSI Tipline specialist creates a record of it in FALCON-TL. The user conducts research in various government, open source, and commercial databases to augment and/or confirm the data in the tip, and enters relevant information in the tip record or uploads the information as an attachment to the tip record. Ultimately, the tip moves to FALCON-SA to be used in the analysis done by other FALCON-SA users. FALCON-TL also includes legacy tips ingested from the ACRIMe Tipline Module.

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

FALCON-TL users may manually query commercial databases subscribed to by many law enforcement agencies, as well as other publicly available websites and social media sites to gather additional information on the suspected illegal activity after a tip is received. For example, suppose the HSI Tipline Unit receives a tip alleging that a terrorist has made threatening statements on his/her Facebook page. If the page is accessible to all Facebook users, the Unit will attempt to verify the allegation and capture an image of the Facebook page containing the alleged threats. The Unit will then analyze the information, conduct additional research, and forward the results to the appropriate HSI field office.

HSI uses this information to help determine if the tip is actionable, i.e., if the tip is sufficiently serious or if enough information exists to warrant the expenditure of investigative resources to follow up on the tip. Obtaining commercially and publicly available information about individuals associated with the tip or other aspects of the tip is helpful to augment the original tip information or attempt to confirm or dispel all or certain aspects of the tip. For example, HSI may use commercial databases to determine that the individual who was alleged to have recently engaged in trade fraud has recently established a business entity engaging in import/export business operating out of a particular state. This information may help the HSI Tipline Unit validate certain information in the tip and provide specific information that the HSI field office can use to begin an investigation.

2.4 Discuss how accuracy of the data is ensured.

The tips submitted to FALCON-TL are provided by members of the public and other law enforcement and government agencies. ICE relies on those providing the tips to provide accurate information but Tipline specialists query various government, open source, and commercial databases along with public websites and social media sites to augment and/or confirm the data provided in tips.

Additionally, restrictions on data modification in the system help to ensure data accuracy. As noted above, when a Tipline specialist creates a tip, he or she completes the report narrative component and FALCON-TL creates the associated report subject properties component. Once the tip record moves into FALCON-SA, the report narrative component can only be edited by Tipline Unit personnel whereas FALCON-SA users are only able to edit the report subject properties component. If a Tipline specialist needs to modify the report narrative component of a tip record in FALCON-SA, the user opens the tip in FALCON-TL and makes the necessary changes, and the changes are instantly viewable by both FALCON-TL and FALCON-SA users. The system's auditing controls capture the changes made to the report narrative component and to the report subject properties component of a tip record thus enabling ICE to know the changes made and the user who made them. By allowing only Tipline Unit personnel to edit the report narrative component and by recording all changes that users make to tip records, FALCON-TL helps to ensure data accuracy.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that information provided about an individual in a tip may not be accurate because the information is provided by a third party and not the individual himself or herself.

Mitigation: Because tips are a report of alleged illegal or otherwise suspicious activities, it would defeat the law enforcement purpose for which they are collected to always contact the individuals being reported in order to verify the information. During the course of an investigation into the tip, ICE agents will use a variety of public and non-public resources to determine the accuracy and reliability of the tip information, including in some cases by conducting an interview with the subject of the tip. Tips are always investigated and verified before the information may be used as the basis for an adverse action against an individual.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

The Tip Information, described in Question 2.1 above, is used by HSI to create a tip record in FALCON-TL and to conduct additional research on the tip. Additional research conducted on the tip, including research in FALCON-SA, is used to confirm, dispel, or augment the information in the tip and to determine whether the tip is actionable and should be referred to the field. As noted above, after it is determined whether a tip is actionable or not, the tip moves into FALCON-SA and is accessible by all

FALCON-SA users.[7] HSI also uses this information to refer tips that are outside of its jurisdiction to the appropriate law enforcement agency for action.

The metadata captured on tips provides additional information about the tips. For example, the metadata captured on tips submitted through the tip form on the ICE public website provides information such as the date and time the tip was submitted and information on the person submitting the information including their IP address, browser information, and Internet service provider. This information may be used when submitting a formal request to the Internet service provider for more information or may be used to obtain evidence in a criminal prosecution.

The reports are used for internal reporting and lead management purposes within ICE.

Tips in FALCON-TL may also be submitted to DHS as part of the Information Sharing Environment Suspicious Activity Reporting Initiative (ISE-SAR). The ISE-SAR is designed to facilitate the sharing of terrorism information among the various agencies that participate and DHS is one of the participating agencies. Tips that are reported in FALCON-TL that deal with terrorism and meet the ISE-SAR requirements will be reported to the DHS ISE-SAR Initiative using the existing process.[8] If the HSI Tipline Unit receives a tip dealing with terrorism that meets the ISE-SAR requirements, the HSI Tipline Unit will forward the information to the Joint Intelligence Operations Center (JIOC) via a Significant Incident Report (SIR) in the ICE Significant Event Notification System.[9] The JIOC will mark the SIR so that the information can be reported using the existing DHS SAR reporting channels.

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.

FALCON-TL does not use technology to conduct electronic searches, queries, or analyses in databases to discover or locate predictive patterns or anomalies. FALCON-SA, on the other hand, does use technology to assist its users in searching, analyzing, and visualizing data to help identify relationships.[10] Tipline Unit personnel conduct additional research in FALCON-SA to confirm, dispel, or augment the information in tips in FALCON-TL.

[7] For more information on the uses of the information in FALCON-SA, see the FALCON-SA PIA.
[8] For more information on the DHS ISE-SAR Initiative, see DHS/ALL/PIA-032 DHS Information Sharing Environment Suspicious Activity Reporting Initiative at http://www.dhs.gov/privacy-documents-department-wide-programs#31.
[9] For more information on the ICE Significant Event Notification System, see DHS/ICE/PIA-023 - Significant Event Notification System (SENS) at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ice_sen.pdf.
[10] For more information on the technology in FALCON-SA used to identify relationships in the information in FALCON-SA, please see the FALCON-SA PIA.

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

No, other DHS components do not have access to FALCON-TL. Only HSI personnel, including contractors and other federal personnel assigned to ICE or to an ICE task force, have access to FALCON-TL.

3.4 Privacy Impact Analysis: Related to the Uses of Information

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

Mitigation: FALCON-TL uses the same access controls, user auditing, and accountability as those described in the FALCON-SA PIA. These protections help to prevent misuse of the information in the system and to identify and support accountability for user misconduct. User activity is audited heavily, including actions such as creating records, modifying records, linking records, searches, and viewing records. ICE has established controls that are based in policy and where possible enforced by technology, and that provide clear instruction on what the authorized uses of the system are. Disciplinary action for violations of ICE policies regarding the system is taken where warranted. Before receiving access to the system, all users are trained on system use and other policies governing the system.

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.

General notice of the existence, contents, and uses of this system are provided by the publication of this PIA and the DHS/ICE-007 ACRIMe SORN, which is being updated separately from the publication of this PIA. Callers to the HSI Tipline Unit hear a message alerting them that they can choose to remain anonymous when providing a tip. Even though a caller chooses to remain anonymous, the HSI Tipline specialist will record the person's phone number. Additionally, the message advises callers that the calls are recorded and that information they provide may be forwarded to the appropriate ICE field office for investigation, as appropriate. For tips collected via the tip form on the ICE public website, there is a Privacy Act statement on the form which informs individuals of the authority, purpose, and sharing (routine uses) of the information being collected. Additionally, the tip form has a link to the privacy policy for ICE's public website which informs individuals about the metadata that the website collects about them. Because the purpose of FALCON-TL is to support the identification of illegal activities and the apprehension of those engaged in such activities, it is not possible to provide notice to the individuals about whom tips are reported.

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

Callers are free to choose what identifying information they provide and if callers request anonymity, it is noted in the tip record created in FALCON-TL. Individuals who submit a tip through the online form also have the option to remain anonymous. They are able to choose what identifying information they provide, but the metadata listed in Section 2.1 including IP address is collected for every tip submitted through the online form. Once the tip is provided to ICE, the person submitting the tip is not afforded the right to consent to how the information provided will be used. Given the law enforcement nature of FALCON-TL, individuals about whom tips are reported are not able to provide consent for how their information will be used or choose to have their information removed from the system.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals about whom tips are reported may not be aware their information may be contained within the FALCON-TL system.

Mitigation: The risk is mitigated primarily by the public notice provided through this PIA and the ACRIMe SORN. Because the purpose of FALCON-TL is to support the identification of illegal activities and the apprehension of those engaged in such activities, it is not possible to provide notice to the individuals about whom tips are reported. Additional notice to the individuals about whom tips are reported is nonexistent because providing such notice could compromise the underlying law enforcement purpose of the system and may put ongoing investigations at risk.

Notice is given to the individuals reporting tips by recorded message on the telephone or using the online form as described above.

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.

HSI proposes to maintain FALCON-TL records for ten (10) years from the date of the tip, to be cutoff at the end of each fiscal year.

5.2 Privacy Impact Analysis: Related to Retention

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

Mitigation: The information in FALCON-TL is proposed to be retained for ten (10) years, which is consistent with general law enforcement system retention schedules and is appropriate given

ICE's mission and the importance of the law enforcement data pertaining to customs, immigration and other violations.

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.

Periodically, the HSI Tipline Unit receives a tip for suspicious activity or suspected illegal activity that is not within ICE's jurisdiction or because of other reasons will not be investigated by ICE, but is otherwise an actionable tip. These tips are entered in FALCON-TL and are then either referred to the appropriate federal, state, local, tribal, foreign or international agency for investigation, or sent to the appropriate ICE field office, which refers the tip to the appropriate agency for action.

Additionally, if a tip is contributed to the DHS ISE-SAR Initiative, the information is available to other authorized agencies that have access to the information. This may include federal, state, tribal, local, international, or foreign law enforcement agencies or other appropriate public or private sector organizations.

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

The sharing of tips with appropriate agencies outside of the Department is compatible with the HSI Tipline Unit's law enforcement purpose described in the ACRIMe SORN. Tips may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. § 552a(b)(3) as shown in the ACRIMe SORN.

6.3 Does the project place limitations on re-dissemination?

There are no limitations on re-dissemination. Limitations on re-dissemination are not appropriate in the circumstances where ICE is referring an allegation of a violation of law to another agency with the authority to investigate and/or enforce that law.

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-TL 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: As mentioned previously, the HSI Tipline Unit periodically receives a tip for an activity that would not be investigated by ICE. The tip is entered in FALCON-TL and then is sent to the appropriate ICE field office. The field office then passes the tip to the appropriate federal, state, local, tribal, foreign, or international agency with the authority to investigate and/or enforce the alleged violation of law. Users are trained to only share tip information with external partners who have a need-to-know the information and prior to sharing the tip with the external partner, the system user completes an accounting for disclosure form in FALCON-SA in order to capture the date, nature, and purpose of the disclosure and the recipient's information.

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-TL, or seeking to contest its content, may submit a request in writing to the 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 an individual access to records contained in FALCON-TL could inform the individual of an actual or potential criminal, civil, or regulatory violation investigation or reveal an 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 an 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 an individual access to records contained in FALCON-TL could inform the subject of an actual or potential criminal, civil, or regulatory violation investigation or reveal an 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 an 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 procedure for submitting a request to correct information is outlined in the ACRIMe SORN and in this PIA in Questions 7.1 and 7.2.

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 this system has a law enforcement purpose, individuals' rights to be notified of the existence of data about them, to review the data to ensure it is correct, 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.

As noted above, once a tip record moves into FALCON-SA, the report narrative component can only be edited by Tipline Unit personnel in FALCON-TL and FALCON-SA users are only able to edit the report subject properties component. The system's auditing controls capture any changes made to the tip record. By allowing only Tipline Unit personnel to edit the report narrative component and by recording all changes made to a record, FALCON-TL helps to ensure data accuracy.

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?

As mentioned before, FALCON-TL is a component system of the larger HSI FALCON environment. As a result, FALCON-TL uses the same access controls, user auditing, and accountability as those described in the FALCON-SA PIA. For more information on these, please see the FALCON-SA PIA.

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

In addition to taking the FALCON-SA training which is described in the FALCON-SA PIA, all FALCON-TL users receive FALCON-TL training. This training includes the rules of behavior, appropriate uses of system data, disclosure and dissemination of records, and system security. Users must complete all training in order to receive authorization to access FALCON-TL. 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-TL as a part of the performance of their official duties will be granted access. An HSI employee's supervisor must submit an access request for FALCON-TL, and the supervisor must validate that the employee has a job-related need-to-know and determine what user role should be assigned. Supervisors submit access requests to designated POCs who validate that the employee meets all the requirements for access to the system, such as the appropriate level of background check. Once this is verified, the FALCON-TL point of contact 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. For contractors, a government employee overseeing the contract will submit user requests and perform the other supervisory roles above.

User roles determine what specific functions users are authorized to perform in FALCON-TL. The basic FALCON-TL user roles are Tipline Specialist, Supervisor, Field Office POC, and System Administrator. The Tipline Specialist is the most basic role and will permit the individual to create, edit, and view tips, and forward them on to supervisors for review. The Supervisor role has the same basic

privileges as the Tipline Specialist user role, plus the ability to review tips, determine if they are "actionable" or not, and to forward them to the HSI field offices. Users with the Supervisor role are also able to view and query audit data, which captures the logon, search, view, create, and forward actions of Tipline Specialist users in the system. The Field Office POC user role enables the user to see and update tips that have been forwarded by a supervisor to the user's field office. The System Administrator role is assigned to those users who administer the system, and grants the user 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 also revoke a user's access when no longer needed or permitted.

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 does not have any information sharing agreements concerning the information in FALCON-TL, nor does it envision the expansion of the systems' users or the intended uses of the information in such a way that any information sharing agreements would be required. In the event that such changes are considered, HSI would engage with the ICE Privacy Office and the Office of Principal Legal Advisor to discuss the intended expanded users and/or uses of this information to ensure that any privacy and legal risks are appropriately vetted. In addition, formal written agreements between ICE and other agencies to share data or provide access to FALCON-TL would be reviewed by the ICE Privacy Office and Office of Principal Legal Advisor as a matter of routine.

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

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security