Privacy Impact Assessment
for the

Firearms, Armor, and Credentials Tracking System (FACTS)

DHS/CBP/PIA-047

August 29, 2017

Contact Point
Christopher Dearie
Program Manager
Office of Information Technology
(571) 468-6133

Reviewing Official
Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP) manages assets and inventory using the Firearms, Armor, and Credentials Tracking System (FACTS). Both CBP and U.S. Immigration and Customs Enforcement (ICE) personnel use FACTS to track and manage serialized assets, non-serialized commodities, job-related training certifications, and inventory. CBP is conducting this Privacy Impact Assessment (PIA) because FACTS collects and maintains personally identifiable information (PII) about employees and dependents of employees deployed overseas.

Overview

Both the U.S. Customs and Border Protection (CBP) and U.S. Immigration and Customs Enforcement (ICE) use the Firearms, Armor, and Credentials Tracking System (FACTS) to (1) provide lifecycle accountability for all aspects of badge, credentials, and firearm inventory; (2) track mandatory firearm proficiency for Agents and Officers, and certifications for firearms instructors; and (3) capture information on firearm maintenance and use of ammunition. FACTS is a web-based application designed to enable users to accept, transfer, and inventory high-risk property in their possession.[1] FACTS manages various types of inventory by tracking the requests for, and distribution of, enforcement equipment from the national CBP armory to the various field/sector armories out to CBP and ICE field personnel. FACTS enables CBP and ICE personnel to process 1) serialized assets, such as firearms, body armor/plate, optics, official identification documents, badges, and credentials; 2) non-serialized commodities, such as ammunition, pepper spray, batons, holsters, and other items that enforcement personnel use in performing their assigned daily duties; and 3) job-related training and certification courses, such as Advanced Firearms Training Exercise, Air Crew Rifle Re-Certification, Firearms Maintenance Training, and other training and certification courses.

The primary functions of FACTS include:

- **General Asset Management Module**: Provides lifecycle accountability for all aspects of badge, credentials, body armor, official passports, and firearm inventory. It identifies each employee with assigned assets and allows employees to inventory these items. FACTS supervisors then verify that the items inventoried are in the employee's physical possession. Features within General Asset Management include:
    - Annual and semi-annual inventory processing. CBP and ICE use FACTS in

[1] FACTS replaced the Firearms Information System (FIS) mainframe system owned by ICE and the Firearms Inventory Tracking system (FITS) owned by CBP. FITS was developed to track all firearms issued to U.S. Customs Service employees, including the employee and organization to whom the weapon was assigned. It also documented certain information about the weapon such as the make, model, serial number, the type of weapon, and its caliber and length. FITS was retired in 2011. All FITS functionality has been incorporated into FACTS.

support of the inventory process. The item's accountable user confirms possession of the inventory in FACTS by adding his or her items for submission to a supervisor prior to manual review and verification. FACTS supports both annual and semi-annual inventory.

- Employee reporting of Lost, Damaged, Destroyed, and Stolen (LDDS) assets and related activity (including tracking of Board of Survey[2] actions and, if applicable, recovery of the item by the asset coordinator);
- Tracking transfers of assets by both asset coordinators and employees;
- Tracking of acquisitions and receipt of new assets, and records requests by asset coordinators; and
- Inventorying, managing, and tracking official passports issued to CBP employees and dependents by the Department of State through the CBP Office of International Affairs (INA). FACTS captures information related to the following passport types: Official, Diplomatic, Official Dependent, and Diplomatic Dependent.

- **Firearm Proficiency Management Module**: CBP and ICE firearm instructors use FACTS to record performance and certification of employee proficiency training, as reported by firearm instructors or defensive tactics instructors.
- **Ammunition Management Module**: Records the complete workflow related to ammunition, beginning with requests by ammunition coordinators; approval by ammunition managers; procurement by Service Level Agreement (SLA) ammunition managers; distribution by SLA ammunition managers to the requesting units; and transfers of ammunition by ammunition coordinators. Firearm instructors also track ammunition usage during training and firearm qualification.
- **Item Repair Management Module**: Armorers at CBP and ICE use repair management to track items in the repair process through initiation, submission, and return. Item repair management maintains a history of each firearm's firing and pins.
- **Credential Creation Module**: Office of Professional Responsibility (OPR) Badge and Credential Coordinators at CBP and ICE use FACTS to create and track physical credentials for current employees, as well as for former employees who are issued credentials in compliance with the Law Enforcement Officers Safety Act of 2004

[2] When a serialized item that is tracked by FACTS gets lost or stolen it is placed into a Board of Survey (BOS) status. The BOS meets once a month to review lost/stolen packets that were submitted by employees. Completion of the BOS process allows for proper review of the circumstances of loss. All BOS actions are supported with a completed loss report (CBP Form 52, Report of Survey).

(LEOSA).[3]

- **Issue Room Module**: Identifies pooled firearms[4] stored in armories and records their issuance to employees at the beginning of their shifts and upon their return.
- **Interface with the Seized Asset and Case Tracking System (SEACATS)**:[5] FACTS interfaces with SEACATS for firearms that are seized and identified for destruction. SEACATS provides FACTS with information in the event that a weapon has been forfeited and is ready to be transferred to the National Firearms Program Staff (NFPS). Once the weapon is ready for transfer from CBP to NFPS, a disposition record is entered in SEACATS and sent to FACTS. FACTS then tracks the disposition record and updates SEACATS once the disposition is completed.
- **Canine Tracking System (K9TS)**: K9TS, a web-based FACTS subsystem, tracks the lifecycle of all CBP canines. The CBP Office of Field Operations (OFO), U.S. Border Patrol (USBP), and the Office of Training and Development (OTD) use K9TS to track the canine procurement, evaluation, training, certification, health/vaccination, and operational activity records.

CBP has developed a mobile application to facilitate asset management in the field or other remote locations. FACTS Mobile provides CBP and ICE users with mobile access to commonly used features of the FACTS web application (*e.g.*, item verification, item inventory, and qualification score capture). Users are able to inventory their assigned serialized items such as firearms, body armor/plate, optics, badges, and credentials. To do so, the employee enters the serial number associated with his or her assigned property; FACTS Mobile then transmits the information to FACTS, which verifies that the person in possession of that item matches the record contained in the FACTS database. FACTS Mobile is not public-facing and only available on CBP and ICE-issued mobile devices.

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?

The information maintained in the system is solicited and obtained under the following authorities: 8 U.S.C. § 1357, *Powers of immigration officers and employees*; 8 C.F.R. § 287.8,

[3] The Law Enforcement Officers Safety Act of 2004 exempts qualified retired law enforcement officers (LEO) from most state and local laws that prohibit the carriage of concealed firearms. LEOSA requires that the law enforcement agency with which the former LEO had been employed assume responsibility for providing its former employee with identification stating that he or she is qualified to carry a concealed weapon as a retired or separated LEO.

[4] Pooled firearms are not assigned to an individual officer, but may be used during a shift.

[5] *See* DHS/CBP-PIA-040 Seized Assets and Case Tracking System (SEACATS), *available at* https://www.dhs.gov/privacy.

Standards for enforcement activities; 8 C.F.R. § 287.9, *Criminal search warrant and firearms policies*; 19 U.S.C. § 1589(a), *Enforcement authority of customs officers*; and 18 U.S.C. 926C(d)(2), *Carrying of concealed firearms by qualified retired law enforcement officers*.

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

FACTS maintains several different types of records covered by the following system of records notices (SORN):

- DHS/ALL-003 Department of Homeland Security General Training Records provides coverage for the collection and maintenance of information used to track and monitor training given to all DHS employees and contractors.[6]
- DHS/ALL-004 General Information Technology Access Records System (GITAARS) provides coverage to collect a discreet set of personally identifiable information (PII) in order to provide authorized individuals access to, or interact with DHS information technology resources, and allow DHS to track use of DHS IT resources.[7]
- DHS/ALL-010 Asset Management Records provides coverage for the collection and maintenance of information used to track all DHS-owned or controlled property that has been issued to current and former DHS employees and contractors.[8]
- DHS/ALL-032 Official Passport Application and Maintenance Records provides coverage for DHS's collection and maintenance of a copy of an official passport application or maintenance record on DHS employees and former employees, civilian personnel, and dependents and family members that accompany members assigned outside the continental United States.[9]

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

Yes. FACTS (CBP-03586-MAJ-03586) received a three-year Authority to Operate (ATO) on August 25, 2014. A revised System Security Plan was completed for FACTS on May 31, 2017, and is compliant with the National Institute of Standards and Technology (NIST) Special

[6] *See* DHS/ALL-003 Department of Homeland Security General Training Records, 73 FR 71656 (November 25, 2008).

[7] *See* DHS/ALL-004 General Information Technology Access Account Records Systems (GITAARS), 77 FR 70792 (November 27, 2012).

[8] *See* DHS/ALL-010 Asset Management Records, 80 FR 58280 (September 28, 2015).

[9] *See* DHS/ALL-032 Official Passport Application and Maintenance Records System, 76 FR 8755 (February 15, 2011). 76 FR 8755.

Publication (SP) Recommended Security Controls for Federal Information Systems (NIST SP 800-53), as well as the DHS National Security Sensitive Systems Handbook and Policy Directive 4300A, version 12.01. CBP is expecting to finalize the re-certification of the FACTS ATO in September 2017, pending completion of this Privacy Impact Assessment (PIA).

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

NARA has issued a number of general records schedules for asset management purposes; however, the CBP Records Management office is currently in the process of reviewing all CBP systems to ensure that the records are aligned with the appropriate schedules. CBP will begin managing FACTS in accordance with general records schedules once they have been approved by the CBP Records Officer, or consistent with any original schedules once they are approved by NARA.

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.

No. None of the information maintained within the FACTS system is collected directly from members of the public, and is therefore not covered by the Paperwork Reduction Act (PRA).[10] The information is provided by employees (including that of their dependents/family members) and is exempt from coverage under the PRA.

[10] Note, however, that forms used by the Department of State for special issuance passports are covered by the Paperwork Reduction Act. Individuals may submit a Form DS-82 or a Form DS-11, depending on individual circumstances. The process for obtaining a special issuance passport differs slightly from the regular passport application process. Individuals who already possess a valid regular passport may be eligible to apply for a special issuance passport using Form DS-82. All other applicants must appear in person before a Passport Application Acceptance Agent or U.S. Consular Officer abroad to submit Form DS-11. Additional information is *available at* https://travel.state.gov/content/sia/en/official-and-diplomatic-passport/how-to-apply/passport-application/first-time-applicant.html.

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.

FACTS collects and maintains only limited employee PII for asset management, firearm proficiency, ammunition and repair tracking, and credential issuance. These functions require only employee name and Hash ID.[11] K9TS also tracks employee/handler email address. In addition, FACTS collects and maintains both CBP and ICE pass/fail information on training and certification courses, qualification scores, and waivers when CBP or ICE personnel are unable to attend a training or perform their qualifications.

In addition to what is listed above, FACTS captures the following information on CBP employees and family members or dependents who are issued official passports for overseas deployment:

- Hash ID[12] of passport holder (which is also applied to any dependents of the employee);
- Full name (first, middle, last);
- Employee's office;
- Passport Number;
- Passport issue date;
- Passport expiration date;
- Date of birth; and
- Passport type (Official, Diplomatic, Official Dependent, and Diplomatic Dependent);[13]

FACTS processes the following information from SEACATS:

- Seizure user ID number (Hash ID);
- Fines, Penalties, and Forfeiture (FPF) number (required);

[11] The HASH ID is an internal identification number created using an algorithm and is based on the employee's Social Security number.

[12] The Hash ID is a unique identifier assigned to CBP employees, derived from the individual's Social Security numbers.

[13] Personal passports are not inventoried in FACTS.

- Line item number (required);
- Sub line number (required);
- Item type;
- Description (required);
- Make (firearm);
- Model (firearm);
- Serial number (firearm);
- Caliber (firearm);
- Unit of Measurement (UOM) ;
- Quantity (required);
- SEACATS item type description (required);
- Shipper;
- Shipping date (required);
- Tracking number;
- Agency code (required);
- Forfeiture number (required);
- Forfeiture date;
- Physical location;
- Creator (required); and
- Create date (required).

FACTS relies upon information from the U.S. Department of Agriculture (USDA) National Finance Center (NFC) for personnel information on CBP and ICE employees. This information includes:

- Hash ID (derived field);
- Organization code;
- Employee name (first, middle, last);
- Agency code;

- Position supervisory code;
- Series code; and
- Position title.

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

In general, information in FACTS is entered by asset managers, asset coordinators, and other individuals responsible for tracking inventory and training. In addition, individual employees may perform actions in FACTS related to the certification of the items in their possession, as well as to report lost or stolen property. FACTS also receives information from external systems, including SEACATS (as described above) and the USDA NFC, which provides a bi-weekly feed of personnel information for all CBP and ICE employees during the pay period cycle.[14]

Regarding passports, CBP INA is the CBP office responsible for coordinating and requesting official passports for CBP personnel and dependents from the Department of State. CBP employees and their dependents are eligible for a "special issuance passport book" since they are either a) an officer or employee of the U.S. Government, traveling abroad for the U.S. Government; or b) the dependent of someone traveling abroad for the U.S. Government, and will accompany them on their assignment.[15] As the travel sponsor, CBP INA initiates the application process with the Department of State. Generally, special issuance passport books are sent to, or picked up by CBP INA, as the sponsor of the employee's official travel. CBP employees and dependents may use the special issuance passport book only when traveling overseas in discharge of the employee's official duties; for personal travel, individuals must use a regular fee passport book or card.

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

No, FACTS does not use data from any commercial or otherwise publicly available sources.

[14] At the end of each pay period, the USDA NFC conducts a Bi-Weekly Examination Analysis and Reporting (BEAR) process. The BEAR process analyzes payroll and personnel transactions that occurred during the processing of the pay period. BEAR sets up the current pay period for payroll- and personnel-related information and closes out the prior pay period. This process is repeated for each pay period. BEAR generates end-of-pay-period report notifications and generates certain personnel actions (*i.e.*, within-grade increase, promotion, name change, etc.). Once that process has completed, the USDA NFC produces files which are referred to as BEAR18 or BEAR download for each of its client organizations.

[15] For additional information about Special Issuance U.S. Passports, please *see* https://travel.state.gov/content/passports/en/passports/no-fee.html.

2.4 Discuss how accuracy of the data is ensured.

FACTS employs the concept of blind verification.[16] For newly acquired assets, the asset manager records each acquired asset based on documents. The armory coordinator records each received shipment independent from the entries of the asset manager. FACTS compares the entries and any discrepancies subject the whole acquisition into "Pending Resolution" by both the asset manager and the armory coordinator. For an item to be counted as received in the inventory, the asset coordinator must physically verify the item.

Certain transactions require approval from authorized roles before they can move forward in a given workflow. For the periodic inventory cycle, the employee inventories his or her assets, which are then physically verified by the supervisory employee and confirmed in the system. Any un-inventoried or un-verified inventoried assets remain incomplete and reported during the inventory cycle period. FACTS provides system level validation features including duplicate data checks and required field checks.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that FACTS may collect more information than is necessary and relevant to accomplish its designated functions.

Mitigation: This risk is mitigated. CBP has determined that FACTS contains the minimal amount of PII necessary to verify the identity of the individual in possession of an inventoried item. Given the sensitive nature of these assets, it is critical that CBP be able to definitively verify the identities of the individuals in possession of these assets at all times to ensure appropriate chain of custody.

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.

FACTS serves as an asset management system which tracks and records purchases, seizures, and distribution of serialized and non-serialized assets from the national armory owners to the various field armory owners for redistribution or for final disposition. FACTS enables CBP

[16] Blind verification is utilized during inventory and the initial recording of new asset acquisition into the system. Blind Verification involves two individuals – one makes the initial entry of a serial number, and another performs the verification of the entry of the first individual. The verifier must have a supervisor role and must enter the serial number of the asset being verified (that is, without the system presenting the actual value entered by the first person). A mismatched entry between the two individuals will place the transaction into a "Pending Resolution" status and must be reconciled. The individual causing the discrepancy will modify the erroneous serial number and is required by the system to enter a textual comment regarding the modification.

and ICE personnel to efficiently process assets classified as serialized firearms, body armor/plate, optics, badges, and credentials. Commodities classified as non-serialized are ammunition, spray/pepper spray, batons, holsters, and other items which enforcement personnel use in performing their assigned daily duties.

The Department of State issues official passports to employees deployed overseas, as well as to spouses and dependent family members who deploy with them. As the government sponsor of the official passport, CBP is responsible for tracking the inventory of official passports sponsored by CBP, including official passports for spouses and dependents of CBP employees deployed overseas. CBP employees and family members deployed oversees are required to use their official passport for all travel related to their international posting with CBP (including travel to and from their duty location, and any other CBP-required travel). CBP also uses passport information to record and manage travel documents according to expiration dates, approved locations, and related data. Employees departing CBP (including on temporary duty military assignments) and employees that have official or diplomatic passports they no longer need or which have expired are instructed to return their Department-issued passports to the CBP Passport and Visa Office by traceable method (*e.g.*, FedEx, UPS). A memo indicating what CBP personnel would like done to the issued passport (*e.g.*, cancel and destroy, cancel and return, or place on file) is included along with the package.

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.

No. No technology is used within FACTS to conduct searches or queries to discover predictive patterns or anomalies.

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

Access to FACTS is limited to CBP and ICE employees and contractors. Specific user roles are based on a determined need to know. Only appropriately cleared personnel, with a valid need to know, supervisor request, owner approval, and least privileges are assigned access roles to FACTS data. Below are the different user roles within FACTS:

1. Employee: Responsible for accepting transfers of items issued to him/her, performing inventory of assigned items, reporting of lost/stolen assigned items, and returning assigned items to asset coordinators when needed;
2. Inventory Specialist (IS): Initiate add and termination of commodities in the field;

3. Coordinator: Conduct inventory of unissued commodity in his/her armories, transfer accountability of commodity to/from employees, initiate repair actions and Lost, Stolen, Tracker/Board of Survey (LST/BOS)/Recovery actions for his/her armories, execute reports;
4. Headquarters Point of Contact: Responsible for management review and approvals of certain documents requiring oversight;
5. Ammo Manager: Responsible for management review and approvals of certain ammunition-related documents requiring oversight, order ammunition for program offices in his/her agency, allocate ammunition lots to program offices, and work with vendors to distribute ammunition to armories;
6. Ammo Point of Contact: Order ammunition for his/her program office and distribute ammunition allocated to his/program office or armory;
7. Manager: Responsible for management review and approvals of documents requiring oversight and enter qualification and training waivers;
8. System Administrator: Ability to perform data modifications to those tables specific to his/her assigned agency, and oversee all aspects of system integrity, perform emergency overrides, initiate inventory and order processing and perform data verification on adding of commodities, and initiate certain transaction documents at discretion of agency administrator;
9. Responsible Official/Co-Authority: Approve commodity requests for his/her organizational authority, verify inventories, run reports against his/her organizational authority, and perform any employee functions because of his/her position of carrying firearms;
10. Supervisor/Verifier: Verify inventories, confirms termination of assets, and oversees specific DHS assets held by external organizations. Designation limited to firearm coordinators, agency supervisors, regional officers (ROs);
11. Firearm Coordinator (FACTS): Conduct inventory of unissued firearms in the field, transfer accountability of commodity to/from employees, and initiate repair actions and LST/BOS/Recovery actions;
12. Firearm Instructor (FACTS): Oversee firearm range qualification sessions and enter qualification scores and waivers, issue ammunition and record its usage;
13. Body Armor Coordinator: Conduct inventory of unissued body armor in the field, transfer accountability of commodity to/from employees, initiate LST/BOS/Recovery actions, and execute reports; and

14. Badge Credential Coordinator: Responsible for receiving, maintaining, and proper distribution of badges and credentials to employees.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a privacy risk of unauthorized access and inappropriate use and dissemination of the information maintained in FACTS.

Mitigation: This risk is mitigated through protection of the PII by role-based access for active users. Personnel requiring access to FACTS are given written authorization from appointed business owner(s). The FACTS application has a robust audit trail that logs action by users and administrators. The system limits access to authorized individuals and warns users that unauthorized, improper use or access to the system may result in disciplinary action as well as civil and criminal penalties. Additionally, all log files are kept for audit and quality control purposes. The logs are audited monthly by the Information System Security Officer (ISSO).

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.

The majority of PII contained in FACTS relates to CBP and ICE employees. Employees in possession of items tracked within FACTS receive notice in the form of direct access to the system for inventory and asset management purposes.

Family members and dependents who have official passports related to a family member's employment with CBP may be aware that CBP maintains their information, but may not have specific notice that their information is retained in FACTS. This PIA provides specific information with regard to the retention and use of their information in FACTS.

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

There is no specific opportunity for CBP or ICE employees and family members of CBP personnel deployed overseas to opt out of their information being maintained in FACTS. CBP and ICE employees consent to their agency's use of their information in general as required in order to perform their duties as employees. Family members of CBP personnel deployed overseas do not have the opportunity to consent or opt out.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: Individuals are unable to consent to the use of their information, decline to provide their information, or opt out of providing their information.

Mitigation: This risk is partially mitigated. Employees consent to provide information to the Department of State for passport issuance when they complete the passport application forms and accept a position with CBP overseas. Employees consent to provide asset and inventory information to the FACTS system as a condition of using government property as part of their official duties. For family members of CBP personnel deployed overseas, this risk cannot be fully mitigated, as they may not opt out of the requirement to provide their information in order to be issued an official passport if they want to accompany their CBP employee family member overseas.

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.

NARA has issued a number of general records schedules for asset management purposes; however, the CBP Records Management office is currently in the process of reviewing all CBP systems to ensure that the records are aligned with the appropriate schedules. CBP will begin managing FACTS in accordance with general records schedules once they have been identified and approved by the CBP Records Officer and NARA.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that data in the various subsystems is maintained longer than needed for business purposes.

Mitigation: This risk is not mitigated. CBP Records Management is in the process of working with the respective program offices to establish appropriate records schedules for these systems. Until a record retention schedule is finalized, all data is retained indefinitely.

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.

No. No information derived from any of the FACTS subsystems is shared outside of the Department.

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

No information derived from any of the FACTS subsystems is shared outside of the Department.

6.3 Does the project place limitations on re-dissemination?

No information derived from any of the FACTS subsystems is shared outside of the Department.

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

No information derived from any of the FACTS subsystems is shared outside of the Department.

6.5 Privacy Impact Analysis: Related to Information Sharing

There are no privacy risks associated with information sharing because no information derived from any of the FACTS subsystems is shared outside of the Department.

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?

Current employees who are authorized users may view their personnel and individual information at any time in FACTS. Former employees and contractors and members of the public may seek access to CBP records contained in FACTS, pursuant to procedures provided by the Freedom of Information Act (FOIA) and the access provisions of the Privacy Act of 1974 by visiting https://www.cbp.gov/site-policy-notices/foia, or may submit a request by mailing the request to:

> U.S. Customs and Border Protection (CBP)
> Freedom of Information Act (FOIA) Division
> 1300 Pennsylvania Avenue, NW, Room 3.3D
> Washington, D.C. 20229

When seeking records about one's self from the system of records associated with this system or any other Departmental system of records, the request must conform to the Privacy Act regulations set forth in federal regulations regarding Domestic Security and Disclosure of Records and Information.[17] One must first verify his or her identity, meaning that one must provide his or her full name, current address, and date and place of birth. One must sign the request, and the signature must either be notarized or submitted under federal statute regarding Unsworn Declarations Under Penalty of Perjury,[18] a law that permits statements to be made under penalty of perjury as a substitute for notarization. While an individual's inquiry requires no specific form, he or she may contact the Chief Privacy Officer and Chief Freedom of Information Officer, https://www.dhs.gov/freedom-information-act-foia, to obtain information on how to submit requests. The request should:

- Explain why the individual believes the Department would have information on him or her;
- Identify which component(s) of the Department he or she believes may have the information ;
- Specify when he or she believes the records would have been created; and
- Provide any other information that will help FOIA staff determine which DHS component agency may have responsive records.

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

If a user notices incorrect information while in the process of receiving an item tracked within FACTS, CBP or ICE personnel can reject the transaction and must provide a comment as to why the item was rejected. The asset managers will correct the data based on proof provided by

[17] 6 CFR part 5.
[18] 28 U.S.C. § 1746.

the user. Former employees or dependents may seek correction of records through the Privacy Act or FOIA processes as described above.

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

Training educates FACTS users on the below methods:

- When an employee is notified by email of a transfer of asset accountability to the employee, the employee is required to log into FACTS. From the employee's homepage notification he or she will see the asset transfer information. If the employee does not accept the accuracy of the transfer record, the employee can reject the transfer of accountability.
- When an employee's training certification or firearm qualification is erroneous, the employee can notify the firearm or defensive tactics instructor of the error, who can then reconcile the discrepancy as necessary.

This PIA notifies former employees and contractors about the mechanisms for accessing their records via the Privacy Act or FOIA and correcting their records in FACTS via the Privacy Act.

7.4 <u>Privacy Impact Analysis</u>: Related to Redress

<u>Privacy Risk</u>: There is a privacy risk that individuals, particularly CBP and ICE, may not know how to access, correct, or amend inaccurate information about themselves in FACTS.

<u>Mitigation</u>: This privacy risk is mitigated. All employees are required to inventory their assets at least once a year in FACTS; through this process, they may access and correct their records. In addition, this PIA notifies former employees and family members of the procedures for access and correction.

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?

FACTS secures data by complying with the requirements of the DHS information technology security policy, particularly the DHS Sensitive Systems Policy Directive 4300A. This handbook establishes a comprehensive program to provide complete information security, including directives on roles and responsibilities, management policies, operational policies, technical controls, and application rules. CBP periodically evaluates FACTS to ensure that it complies with these security requirements.

Additionally, FACTS employs technical controls, including role-based access and audit logs to ensure that the information is used in accordance with the stated practices in this PIA. CBP also performs a periodic assessment of physical, technical, and administrative controls to enhance accountability and data integrity.

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

All FACTS users are required to take several mandatory courses that address protecting PII, system security, and online rules of behavior. Specific mandatory online training includes:

- CBP IT Security Awareness and Rules of Behavior Training;[19] and
- Privacy at DHS: Protecting Personal Information.

Completion of the annual privacy and security training ensures that CBP FACTS users have a sufficient understanding of proper handling and safeguarding of PII. Failure to complete the course results in the removal of access to the system.

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

Access to information in FACTS is role-based, and granted on a "need to know" basis determined by duties. FACTS System Administrators assign roles and authority ranges.

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?

Information contained in FACTS is not shared outside of CBP. Given that FACTS serves as an asset management system, no users outside DHS have access to FACTS. In general, all information sharing and information sharing agreements must be reviewed and approved through an internal CBP process, which includes a review by the policy and privacy teams, as well as legal counsel.

8.5 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk: There is a privacy risk that individuals may have unauthorized access to the information maintained in FACTS.

[19] ICE users take an equivalent training called "ICE Information Assurance Awareness Training (IAAT)."

<u>Mitigation</u>: To mitigate this risk, CBP employs role-based access controls so that authorized users have only the access they need in order to perform their functions. Only users with a "need to know" may access FACTS; together with the principle of least privilege, a CBP FACTS Business Owner determines what features in FACTS the user will access. Only System Administrators and users with update roles can access and change fields in the system. Additionally, all users of FACTS user accounts must conform to appropriate security and privacy policies, follow established rules of behavior, and be adequately trained regarding the security of their systems. CBP also performs a periodic assessment of physical, technical, and administrative controls to enhance accountability and data integrity.

Responsible Officials

Christopher Dearie
FACTS Program Manager
Border Enforcement and Management Division
Office of Information Technology
U.S. Customs and Border Protection

Debra L. Danisek
CBP Privacy Officer
Office of Privacy and Diversity
U.S. Customs and Border Protection

Approval Signature

<u>Original, signed copy on file at the DHS Privacy Office.</u>

____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security