Privacy Impact Assessment
for the

FPS Post Tracking System (PTS)

DHS/FPS/PIA-003

September 20, 2019

Contact Point
Curtis Purintun
Post Tracking System
Federal Protective Service
Cybersecurity and Infrastructure Security Agency
(202) 732-8151

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

Abstract

The Department of Homeland Security's (DHS) Federal Protective Service (FPS) is developing the Post Tracking System (PTS). PTS will be used to verify the identity, suitability, training completion, and time and attendance of Protective Security Officers (PSO) who serve as contracted guards at federal facilities. FPS is conducting this Privacy Impact Assessment (PIA) because PTS collects personally identifiable information (PII) of DHS employees and contract personnel.

Overview

FPS[1] is charged with providing security and law enforcement services to approximately 9,000 federal facilities owned or leased by the General Services Administration (GSA). FPS's mission is to protect the buildings, grounds, and properties that are owned or leased by GSA and other federal agencies, and the people who work within and visit them. FPS enters into contracts with various companies employing more than 13,000 PSOs to stand post and protect numerous facilities nationwide.

FPS currently has a paper-based, manpower-intensive, and time-consuming process in place to manage PSOs who are assigned at various locations. The current PSO management process relies heavily on contractor self-reporting, and it is supported by technology (to the extent that the process is automated) that has significant capability gaps. Therefore, FPS has identified mission functions that must be executed to better manage its PSO program, such as:

- The ability to remotely confirm that guard posts are staffed as required;
- The ability to verify PSO certifications and suitability findings to ensure that FPS posts are staffed by qualified and cleared PSOs;
- The ability to automatically gather and store PSO management data needed to validate contract invoices, respond to data calls, provide management reports, and analyze performance; and
- The ability to verify time and attendance of PSOs.

How PTS will Operate:

The proposed PTS will prove beneficial from a user perspective. The expected sign-in process will include a suite of backend services, such as the use of multi-factor authentication

[1] On November 16, 2018 the President signed into law the Cybersecurity and Infrastructure Act, which established the Cybersecurity and Infrastructure Security Agency (CISA) and authorized the transfer of FPS to a component, directorate, or other office of the Department of Homeland Security (DHS) that the Secretary determined appropriate. On October 1, 2019, FPS will become part of DHS Headquarters under the Management Directorate.

(DHS Personal Identity Verification [PIV], Personal Identification Number [PIN], and scanning of fingerprint).

The sign-in process will require three-factor authentication. PSOs will insert their PIV card into the handheld card reader, they will then enter their PIN, and lastly, they will place their fingerprint on the HSPD-12-compliant fingerprint reader.[2] The fingerprint will be read from the fingerprint reader and compared to the image stored on the PIV card. The fingerprint is not stored within PTS (just as a PIV/PIN are not stored to a system when personnel unlock their computers), as its purpose is to serve as an authentication measure. The fingerprint scan is discarded as soon as it is matched with the fingerprint stored on the PSO's PIV card.

The PSO contract vendors will supply the on-site PIV/fingerprint reader; the device will not be supplied by FPS itself. PTS will use PIV cards as a form of PSO identification and as a means for them to sign in to their respective posts. PSOs will abide by the guidelines on PIV usage as communicated by DHS policy. PTS will verify PSOs' data, to include suitability and training certification, and facility information from the following systems:

- FPS PSO certification management system (FPS Training and Academy Management System [TAMS][3]);
- Integrated Security Management System (ISMS),[4] which provides suitability, clearance, and citizenship data via TAMS; and
- FPS's facility management system (currently FPS's Modified Infrastructure Survey Tool [MIST 2.0][5]).

For example, if a location requires a PSO to be certified in Firearms, Cardiopulmonary Resuscitation (CPR), and First Aid, PTS will receive these requirements from the systems listed above. If the PSO does not meet these requirements, the individual will not be able to stand post unless he/she gets a waiver from the Contracting Officer Representative (COR).

---

[2] Homeland Security Presidential Directive 12 (HSPD-12) is a policy for a common identification standard for federal employees and contractors. *See* Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors (Aug. 27, 2004), *available at* https://www.dhs.gov/homeland-security-presidential-directive-12.

[3] *See* DHS/NPPD/PIA-024 FPS Training and Academy Management System, *available at* https://www.dhs.gov/privacy.

[4] *See* DHS/ALL/PIA-038 Integrated Security Management System (ISMS), *available at* https://www.dhs.gov/privacy.

[5] MIST is the protective tool suite used by FPS to systematically capture, store, and access information associated with federal facility within its area of responsibility. Data in the system includes threats, vulnerabilities, occupants, countermeasures, security plans, and other relevant information. Limited PII is collected on users to provision accounts.

PTS will be used by PSO and non-PSO user groups either through an On-Site Handheld Device (OHD)[6] or web application. PSO users include both PSOs and PSO Supervisors who will access PTS via an OHD. The PSOs stand post and use the device to check in and out in order to record that the post is staffed. PSO Supervisors are the first-level managers of the PSOs who provide oversight and management and may, at times, stand post. Non-PSO users include FPS Inspectors, CORs, IT Administrators, and Helpdesk personnel. They will access PTS via the web application to confirm that posts are appropriately staffed, gather data, validate invoices, generate reports, and resolve and troubleshoot alerts or system errors. Non-PSO users will use two-factor authentication, via PIV and PIN, to access PTS.

Like most systems, basic business contact information will be used to establish records/profiles within PTS so that alerts can be sent and basic user management can be conducted. This information will be collected for all FPS users, including FPS Managers (Area Commanders and District Commanders), Inspectors, Contract Administrators, (CORs, Contracting Officers [COs], PSO Program Managers, Contract Specialists, Resource Management Branch Chiefs, and Threat Management Branch Chiefs), Help Desk Representatives, IT Administrators, and Super Administrators (Protective Security Operations Division [PSOD], Technical Security Specialist, and Information Technology Division [ITD]).

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?

DHS is authorized to collect this information pursuant to:

- 5 U.S.C. § 4103, Establishment of training programs;
- 5 U.S.C. § 4302, Establishment of performance appraisal systems;
- 5 CFR Part 410, Training;
- 5 CFR Part 430, Performance Management; and
- 40 U.S.C. § 1315, Law enforcement authority of Secretary of Homeland Security for protection of public property.

[6] An OHD is a tablet or laptop that meets PTS operating requirements, including three-factor authentication (PIV card, associated PIN, and fingerprint). PSOs use OHDs to access the PSO user interface of PTS, while non-PSO users use the web application. OHDs do not store any PII or any of the data associated with PTS.

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

The information collected in PTS is covered by the following system of records notices (SORN):

- DHS/ALL-003 Department of Homeland Security General Training Records;[7]
- DHS/ALL-021 Department of Homeland Security Contractors and Consultants;[8]
- DHS/ALL-024 Facility and Perimeter Access Control and Visitor Management System of Records;[9] and
- DHS/ALL-026 Department of Homeland Security Personal Identity Verification Management System.[10]

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

The PTS Authority to Operate (ATO) is expected to be granted upon completion of this PIA.

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

PTS will retain contractor PSO personnel records relating to post assignments, suitability to stand post, and time and attendance. The National Archives and Records Administration (NARA) has established General Records Schedule (GRS) for these records. The following GRS schedules are applied accordingly:

- GRS 5.6 item 010 Security Administrative Records - PSO assignment records
    - Records are destroyed when three years old.
- GRS 5.2 Transitory and Intermediary Records - Official records for background/suitability and training records obtained through ISMS and TAMS
    - Records are destroyed when no longer needed.
    - When a PSO is no longer employed by a contractor, his or her information is no longer provided in data uploads, and the user account and user records are automatically disabled and removed during the data upload process.

[7] *See* DHS/ALL-003 Department of Homeland Security General Training Records, 73 FR 71659 (Nov. 25, 2008).
[8] *See* DHS/ALL-021 Department of Homeland Security Contractors and Consultants, 73 FR 63179 (Oct. 23, 2008).
[9] *See* DHS/ALL-24 Facility and Perimeter Access Control and Visitor Management System of Records, 75 FR 5609 (Feb. 3, 2010).
[10] *See* DHS/ALL-026 Department of Homeland Security Personal Identity Verification Management System, 74 FR 30301 (June 25, 2009).

- GRS 2.4 item 030 Time and Attendance Records - PSO time and attendance records.
    - Records are destroyed after GAO audit or when three years old, whichever is sooner.

FPS will annually review the records retained and ensure they are stored in accordance with the approved retention schedule. PSO user records for PSOs no longer on the contract are deleted during the ISMS uploads.

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 information requested and stored in PTS is only collected from employees and contractors working for FPS. Therefore, the Paperwork Reduction Act (PRA) does not apply to this collection.

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.

PTS collects information from PSOs and non-PSOs (FPS Managers, Inspectors, CORs, FPS Contract Administrators, Help Desk Representatives, IT Administrators, and Super Administrators). FPS will review annually the data the system collects to ensure the system continues to collect the necessary data. The following data is collected and stored within PTS:

- Name (First name, Middle initial, Last name) (All PTS users);
- Post Staffing Assignments (e.g., Officer John Doe is to work the loading dock post at 800 N. Capitol St.) (PSOs only);
- Contract, Contract Line Item Number (CLIN), and Post (PSOs only);
- Required Post Hours (PSOs only);
- PSO Qualifications (e.g., clearance, certifications obtained and currently held by the PSO such as Firearm carrying license, Driver's license, CPR certification) (PSOs only);
- Facility Name and Locations (PSOs only); and

- System Log reports (System Logs record all system activity associated with the OHD and web application. For example: all log-in/out attempts by PSOs, system events, alerts, and waivers. No additional PII is included in these reports.) (All PTS users).

PTS will interface with FPS TAMS to provide the certification and training qualification for the PSOs and will also retrieve suitability, clearance, and citizenship data from ISMS through TAMS. The PTS/TAMS interface will provide qualification data depicting all the training and certifications the PSO has obtained. This qualification data will be used by PTS to determine if the PSO qualifications match the post requirements. These associations allow FPS to determine if PSOs are qualified to stand post. The data extract from TAMS and stored in PTS will include the following for each PSO qualification:

- PSO's Electronic Data Interchange Personal Identifier (EDIPI), a unique identifier;
- PSO's First Name, Middle Name, and Last Name;
- Citizenship (derived from ISMS via TAMS);
- Contract Number, Contractor Company (derived from ISMS via TAMS);
- Clearance Type, Condition, and Status (derived from ISMS via TAMS);
- Qualification Type and Name; and
- Qualification Start (issued) and End Dates.

The PTS/MIST interface will associate PSO post information with facility information, allowing the system to incorporate post and facility locations, security levels and requirements of the facilities and posts, and other related information. The system will be able to see the posts at each facility and the location of each facility. In addition, this will allow the system to associate security and law enforcement requirements to stand post to a specific facility and post. PTS only extracts facility information, not PII, from MIST.

The data extracted from MIST and stored in PTS will include the following for each facility:

- Unique building identification (ID);
- Proper name and street address of the facility;
- FPS region, district, and area that the facility is within;
- Designation of whether the facility is active or not with respect to GSA leasing; and

- Facility Security Level (FSL).[11]

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

PSO identity is determined through direct user input via PIV cards, PINs, and fingerprints. This information is not stored in PTS, but merely validated in a similar way to an employee entering credential information when logging on to his/her computer.

The type of information captured in PTS is user identity, post information, post hours, and PSO certifications. This information is input directly into PTS (either manually or through data imports) by FPS CORs who have access to the appropriate PSO contract information. Post hours, staffing requirements, and all PSO requirements are delineated in PSO vendor contracts.

PTS will verify PSO suitability from information that originates in ISMS, and PTS receives the data via the TAMS interface to PTS. This data will be used to validate the eligibility of the PSO to stand post. This validation will occur by searching the data attributes associated with the PSO's EDIPI and PSO vendor information.

PTS will verify the PSO training and accreditation information from TAMS in order to validate the PSO's training and certifications are up to date. PTS will verify the facility information from the MIST application for the updated list of all facilities requiring PSO staffing.

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. PTS does not use information from commercial sources or publicly available data. All PTS data is derived from internal information sources such as TAMS, ISMS, and MIST, and directly from the individual user.

2.4 Discuss how accuracy of the data is ensured.

The information in PTS is assumed to be accurate because it is collected from reliable internal DHS/FPS systems, and directly from the individual when applicable. In addition, PTS will rely on the reviews of PTS-generated reports by FPS CORs and Protective Security Officer Program Managers (PSOPM) for accuracy. Multi-level reviews and verification of the data will occur as a form of checks and balances for data integrity. If data is found to be inaccurate, appropriate action, verification, and correction of data will take place. If for any reason PTS finds

[11] The FSL determination ranges from a Level I (lowest risk) to Level V (highest risk). For more information on FSLs, *see* Public Building Service (PBS) Leasing Desk Guide, Chapter 19: Security (Sept. 28, 2012), *available at* https://www.gsa.gov/cdnstatic/LDG-Chapter19_9-28-12_final_508.pdf.

the PSO unqualified to stand post, the PSO can work through his/her supervisor, COR, or vendor program manager (PM) to correct any data inaccuracy in the system of record.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that PTS could collect and store more data than is needed to achieve its mission functions.

Mitigation: The risk is mitigated. Only the minimum information is collected to perform the required functions of PTS. FPS has reviewed all data fields to determine the minimum amount of information required for the system to operate. All fields in other connected systems were analyzed to determine their utility to the mission of PTS, and only necessary and required information is collected from other systems. FPS will review annually the data the system collects to ensure PTS continues to collect only the minimal amount of PII necessary.

Additionally, PII is only stored in PTS and no PII data will be stored on the OHDs.

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.

FPS uses PTS to monitor and ensure the performance of PSOs. FPS will use the information gained through the authentication and validation of each PSO to conduct the six key processes below:

1. Authenticate the identity of the PSO before he or she staffs the post;
2. Confirm the PSO is properly trained and currently certified to stand post;
3. Confirm the PSO is currently suitable (cleared) to stand post;
4. Document each individual PSO's productive post hours staffed;
5. Determine which posts are unstaffed or staffed by unqualified PSOs, and FPS managers generate a report to notify the PSO Vendor PM of an unqualified and unmanned post; and
6. Report on the productive hours worked by all PSOs within a contract, so that this information can be used to review and validate invoices received from PSO vendors.

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. PTS will use technologies to conduct report queries and conduct analysis on PSO performance, but the system will not be used to predict a pattern or anomaly.

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

PTS will only be used by FPS personnel and contractors. No one else outside of FPS will have assigned roles or responsibilities within the system.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that PSO performance data (e.g., PTS reports on post hours worked or variance to expected post hours) may be mishandled and made available to unauthorized persons.

Mitigation: The risk is mitigated. PTS users will have role-based access based on their position within FPS. The Super Administrator will assign access to users based upon their defined job titles. Only authorized personnel (e.g., FPS Managers/Auditors and FPS CORs) will have access to PSO performance data. Additionally, PSOs are required by contract to annually take and pass the DHS privacy training.[12]

The inability for an unauthorized user to access this data has been tested thoroughly during the development phases of PTS and will continue to be monitored. All access attempts will be tracked, monitored, and reviewed using system logging.

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 information collected by PTS is done so from an authorized system user, either a PSO who knowingly enters his/her information or a non-PSO or FPS supervisor who received that

[12] For more information on DHS security and training requirements for contractors, *see* https://www.dhs.gov/dhs-security-and-training-requirements-contractors.

information from the PSO or PSO's company or DHS systems (e.g., TAMS, ISMS).

This PIA and the applicable SORNs also provide notice of the intent to collect this type of information. No information on the general public is collected, only on current FPS federal employees and contractors.[13]

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

Due to the law enforcement purpose of the system, there are no opportunities for a PTS user to decline to provide his/her PII. PSO performance and related post and staffing information will be tracked in the automated system once PTS is in production. Choosing not to enter information into the system will inherently disrupt the ability to monitor PSO personnel and their associated contracts. However, it should be noted that only the information that is required to be monitored will be captured in PTS; no additional personal information will be gathered or collected.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that the individual will not have prior or existing notice of the collection of his/her information in PTS.

Mitigation: This risk is mitigated. Individual PSOs know they are inputting their post information (e.g., post hours) into PTS because they have to log in to the system to do so. PTS also uses information provided by the contract employer or DHS systems (e.g., TAMS/ISMS) that the individual PSO would have had to provide previously. Notice is provided through the publication of this PIA and related SORNs, as well as Privacy Act Statements provided to personnel when they are granted PIV cards for access to DHS facilities. In addition, mandatory PTS training will explain which data elements are captured by PTS so all authorized users, including PSOs, are fully aware of the collection of the information.

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.

FPS follows a record schedule according to GRS that meets the unique collection of records in PTS. The retention schedule will follow existing timelines, specifically GRS 5.6 item 010 for PSO assignment records, GRS 5.2 for official records for background/suitability and training

[13] FPS users must accept a system user agreement before entering PTS. PSOs do not directly access the system when checking in and out of the OHDs and therefore do not have to accept a system user agreement.

records obtained through ISMS and TAMS, and GRS 2.4 item 030 for PSO time and attendance records.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that information will be retained for longer than is required or needed in PTS.

Mitigation: The risk will be mitigated by applying applicable, existing GRS record schedules. FPS will review the record schedules and information collected annually, and the system will dispose of records in accordance with a NARA-approved records schedule.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information shared 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 information will be shared outside of DHS as part of the normal agency operations.

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

No information will be shared outside of DHS as part of normal agency operations.

6.3 Does the project place limitations on re-dissemination?

As stated in Sections 6.1 and 6.2, this information will not be shared outside of DHS as part of normal agency operations.

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

PTS is an FPS-specific system and will not exchange or share information outside of the Department. If a request is made by a contractor for its respective PSO records, FPS will maintain an accounting of all such manual disclosures, which will be kept on file at the FPS Protective Security Operations Division (PSOD).

6.5 Privacy Impact Analysis: Related to Information Sharing

There is no risk related to information sharing because no information is shared outside of FPS.

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?

PTS is a system that relies partially on outside systems for the data it collects. Much of the data listed in Section 2.1 is maintained by the vendor company (i.e., the PSO's employer). Additional systems, such as TAMS and MIST, are used to verify eligibility and suitability data. The PSOs will see end results; however, they will not interface with their information daily. Instead, PTS will simply validate the PSOs' eligibility to stand at that post.

A PSO can inquire about the information sent to PTS with his/her employer if the PSO believes information to be inaccurate or erroneous. Access to individual information in TAMS and MIST will be done in accordance with procedures established by those systems. The PSO will work through his/her immediate supervisor and COR to access this information.

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

If a PSO finds information to be inaccurate, the PSO can contact his/her supervisor, as directed by the system and training. The supervisor will contact the FPS COR to determine from which system the information was pulled. The FPS COR will then notify the owner of that system of record to correct the information. For example, TAMS data is maintained, and must be corrected, by the vendor, and MIST data is maintained and corrected by FPS.

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

The PSO is directed by the system and through training to contact his/her immediate supervisor and employer when failing verification of eligibility and suitability that may have resulted from incorrect information.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that a PSO finds information within PTS that is inaccurate and does not understand the redress processes.

Mitigation: The risk is mitigated. FPS will follow the process and procedures described in Section 7.2 to resolve any discrepancies reported. FPS ensures PSOs understand the redress processes through the system and training. PTS will provide on-screen messages through the OHD

to the PSO when the underlying data identifies that the PSO is determined not to have the appropriate credentials to stand post. The underlying data is provided and maintained by the PSO vendors. It is not only the PSO vendor's responsibility to provide and maintain the data but also to certify and train PSOs relevant to all credentials to stand post. PSOs are also instructed through training to contact their supervisors (PSO vendor) relevant to these messages.

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?

PTS uses technical controls to ensure that information is used in accordance with the stated practices in this PIA. The system controls access to specific PTS functions by assigning roles to each user. System administrators have full access to PTS and are tasked with assigning these roles to individual users. Every individual user who has access to PTS will require a DHS PIV card that will be used to log in to the system. PTS will also have full audit capabilities to track data changes in the system.

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

DHS provides required annual privacy and security awareness training to all employees and contractors, which equips them with information on safeguarding PII. DHS also requires that all PTS users complete PTS user training or PTS privileged user training prior to using the system and annually.

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

PTS users must have an official need for system information to complete their duties. System administrators will be in charge of assigning each user group, including FPS Managers (Area Commanders and District Commanders), Inspectors, Contract Administrators (CORs, Contracting Officers [COs], PSO Program Managers [PSOPMs], Contract Specialists, Risk Management Branch Chiefs, and Threat Management Branch Chiefs), Help Desk Representatives, IT Administrators, and Super Administrators (Protective Security Operations Division [PSOD], Technical Security Specialist), with roles that limit access to the basic functions required to

perform their duties. Permissions can be modified upon request for individual users who have a need for expanded roles.

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

Except for reports and audits, PTS information is necessary only within DHS. When outside agency request access to or information from PTS, these requests will be reviewed by FPS Management, the PTS Program Manager, System Owner, Information System Security Officer (ISSO), and DHS Privacy Office. Requests for PTS access from internal DHS organizations other than FPS will be reviewed by the same groups and people stated above.

Responsible Official

L. Eric Patterson
Director, Federal Protective Service
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