Privacy Impact Assessment Update
for the

Protective Threat Management System

(PTMS)

DHS/USSS/PIA-003(a)

July 2, 2019

Contact Point
Zachary Ainsworth
Senior Intelligence Advisor
U.S. Secret Service
(202) 406-5731

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

Abstract

The United States Secret Service (Secret Service or USSS) Protective Threat Management System (PTMS) is a case management system used to record information required to assist the agency in meeting its protective mission. PTMS records data on potentially threatening behavior and incidents that may impact the USSS mission to protect persons, events, and facilities. USSS uses data from PTMS to develop threat assessments. This PIA Update is being conducted to document the addition of a new subsystem called Uniformed Division Log Book (UDLB) to the PTMS system infrastructure, and new information sharing with USSS systems: Applicant Lifecycle Information System (ALIS), Electronic Check (eCheck), and Enterprise Person (ePerson).

Overview

The USSS protective mission includes the protection of the President, Vice President, their immediate families, former Presidents and Vice Presidents, major candidates for the presidency and vice presidency, foreign heads of state visiting the United States, and other individuals, events, and places authorized to receive Secret Service protection. To meet its protective obligations, the USSS maintains records in PTMS that include personally identifiable information (PII) on individuals expressing threatening or inappropriate behavior and on other incidents that may impact the Secret Service's mission to protect persons, events, and facilities. The Secret Service defines a threat as any form of communication (written, electronic, verbal, or non-verbal) that meets the elements of Title 18, United States Code, Sections 871 or 879, or other appropriate federal or state statutes. Other incidents for which records are created vary widely and may include overflights of restricted airspace, civil disorder, exclusions from sites, natural occurrences, bomb incidents or hoaxes, hijackings, incidents affecting motorcade movements, security compromise, uncorroborated source reporting, assassination or attempts, and other incidents judged to be of interest to protective operations.

PTMS includes features such as workflow record keeping, ability to add new data fields to reflect changing requirements, the ability to attach electronic documents, enhanced text searching capability, the ability of some users to construct queries combining any number of PTMS data values with data-appropriate operators and, since PTMS is a web-based application, improved access for field users with a need-to-know.

PTMS mostly houses case records on investigations initiated by the Secret Service, but may also contain case records that contain information received from other government agencies and created through their own investigative efforts. This information is shared with the Secret Service to assist in accomplishing its protective mission. Such cases may relate to a terrorist organization, a homegrown violent extremist, or an individual(s) engaged in targeting U.S. Government officials or facilities. PTMS also maintains cases containing non-investigative information. Examples of such information would include lost or stolen Secret Service property,

and information about incidents that, while not threatening, may have affected a protectee's movement or protected event.[1]

PTMS does not include information on individuals merely seeking access to protected facilities or sites unless they were excluded from a protected site or come to the attention of the Secret Service for threatening, inappropriate, or unusual behavior. Subjects may come to Secret Service attention through direct contact, violent or threatening social media posts made in public forums, reports from concerned citizens, other agency reports, or media reporting. Information acquired through those means is evaluated by personnel trained in threat assessment protocols and may include: physical identifiers, criminal history, health history, employment history, military service history, education history, immigration status, and other personal information provided by the subject or others familiar with the subject. PTMS does not perform biometric analysis.

Information from PTMS is used to develop threat assessments to assist protective operations personnel in creating a secure environment for Secret Service protected persons, events, and facilities. A threat assessment offers a description of the current threat environment for those individuals or events protected by the Secret Service. Use of PTMS is restricted to personnel who need information to effectively perform their job functions. Examples of typical transactions would be a user entering information to reflect the office assigned an investigation, typing a text summary of an investigation, establishing a new case record, or establishing a report to record initial receipt of information. When establishing a new record, minimum information is required from the user that may include a case title or subject name (and if a subject, then also minimum physical identifiers), the employee(s) and office assigned to the case, and whether or not a physical file is kept.

PTMS records are established to record initial receipt of information (intake) from a source and what actions were immediately taken. If the information is investigated, then a Protective Intelligence and Assessment Division (PID) user establishes a case record that contains the activities and results of the investigation. Other cases may be established to record incidents of protective interest because they occurred at a protected site or effected a protected movement. Related source documents may also be attached electronically to the PTMS record.

An example of a typical query is an authorized user entering query criteria to identify a subject by name. Users search for subject records, based on PII, whenever a subject comes to Secret Service attention through direct contact, violent or threatening social media posts made in public forums, concerned citizens, other agency reports, or media reporting. Direct contact may include individuals seeking access to protected facilities or events.

Headquarters users in PID enter data into PTMS through use of a computer interface. PID users have wide-ranging system rights to create and edit PTMS records. Only a small number of

[1] 18 U.S.C. § 3056, as amended, "Powers, authorities, and duties of the United States Secret Service;" 18 U.S.C. 3056A "Powers, authorities, and duties of the United States Secret Service Uniformed Division."

PID users have systems rights to retire or purge PTMS records. PID users may conduct queries for information based on PII or other administrative characteristics of the case, such as employee assigned, open and close dates, dates of judicial action, protectee, type of incident, or date of activity. They use queries of PTMS to:

- Identify individuals who have previously threatened or expressed an inappropriate interest in a particular protectee(s);
- Identify individuals who have previously come to the attention of the Secret Service;
- Identify suspects for investigations in which the subject is unknown;
- Report administrative case information to Secret Service management officials; and
- Report statistical case information to Secret Service management officials, the Department of Homeland Security, Office of Management and Budget, and the U.S. Congress.

Field and certain headquarters users not assigned to PID may also access PTMS, but have limited or no system rights to edit records. These users are also restricted to viewing only those portions of records that are needed to confirm an identity, location, or provide for employee safety. PTMS records (and information entered into them) must be manually entered with the exception of the user name when establishing new records and certain date/times related to record creation or updates. PTMS does not connect to external systems. PTMS records are not automatically updated and cannot be manually updated without an authorized user accessing PTMS.

Access to PTMS is strictly limited to authorized Secret Service employees who have a need to know in the furtherance of their role in protective intelligence analysis. User access to PTMS is controlled by role-based permissions and includes various levels depending on the user's function in USSS. The most restricted level of access is granted to special agents (who investigate individuals expressing threatening or inappropriate behavior and other incidents that may impact the agency's mission to protect persons, events, and facilities) and field-based administrative personnel who record administrative case information in PTMS (e.g., case agent name, an arrest date, or case disposition). Staff assigned to PID at USSS headquarters are granted additional access, allowing these users to create and edit report/case records. The least restricted level of access is granted to certain supervisors in PID who may retire or purge entire case records, edit the pre-populated values available for users to select in list-of-value fields in PTMS (e.g., the state field of an address record), create and edit names and titles of protected persons, and manage the permissions allowed at any level of user access.

Reason for the PIA Update

The reason for this PIA Update is to document the addition of the new subsystem, Uniformed Division Log Book (UDLB), which serves as a tool to monitor, track, and report on Uniformed Division (UD)-related incidents that occur at each of the five supported branches:

White House, Foreign Missions, Naval Observatory, Office of the Chief, and Special Operations. There is also an interconnection between PTMS and the following USSS applications: Applicant Lifecycle Information System (ALIS),[2] Electronic Check (eCheck),[3] and Enterprise Person (ePerson).[4]

Privacy Impact Analysis

Authorities and Other Requirements

There are no changes in the specific legal authorities and agreements that permit and define the collection of information in PTMS.

Characterization of the Information

The PTMS UDLB subsystem collects information on suspects when a Uniformed Officer makes an arrest, and information can also be captured for a sick or injured individual the Uniformed Officer comes into contact with. The UDLB subsystem can collect and/or process in various combinations, depending on the justification for entry, one or more of the following:

- Name (First Name, Middle Name, Last Name);
- Street;
- City;
- State;
- Home Phone;
- Office Phone;
- Social Security number (SSN);
- Date of Birth (DOB);
- Nationality;
- Gender;
- Height;
- Weight;
- Race;

[2] DHS/USSS/PIA-023 Applicant Lifecycle Information System (ALIS), August 2018, https://www.dhs.gov/sites/default/files/publications/privacy-pia-usss-alis-august2018.pdf.
[3] DHS/USSS/PIA-012(b) Electronic Name Check System, September 2016, https://www.dhs.gov/sites/default/files/publications/privacy-pia-usss-echeck-september2016.pdf.
[4] DHS/USSS/PIA-016(a) Enterprise Person (ePerson) System, June 2018, https://www.dhs.gov/sites/default/files/publications/privacy-pia-usss-eperson-june2018.pdf.

- Hair color;
- Eye color;
- Branch Sector;
- Hate Crime;
- Drug Arrest;
- Violent Crime;
- Gun Crime; and
- Arrest Charges.

UD personnel also capture and enter incident data on alarms, assistance to the embassies/other agencies, coverage, demonstrations (no names captured unless arrest made), employee sick and injury reports, penetrations, threats, and vehicle accidents into the UDLB subsystem. All incidents documented are those that have taken place at or near a location that UD personnel provide protective services. Data recorded includes:

- UD reporting staff member;
- UD reporting branch;
- Incident type;
- Incident location;
- Incident date/time;
- Approver info;
- Injury detail (if applicable); and
- Uploaded copy of the printed report.

The module allows users to change the status of the incident, add supplementary information, and record suspects as appropriate. UDLB generates statistical reports and provides a robust search mechanism.

The interconnections to/from ePerson, ALIS, and eCheck enable the following:

PTMS uses Oracle database links to communicate to the ePerson database for purposes of: 1) determining the appropriate USSS district office when a user supplies a city and state; 2) querying for USSS personnel identified as agents; and 3) granting USSS agent personnel access to discrete PTMS functionalities.

ALIS and eCheck query the PTMS database to determine if a USSS job applicant or National Special Security Event (NSSE) attendee has an open case, or is a person of interest by PID. The queries conducted by the ALIS and eCheck systems include the following:

- First Name;
- Last Name;
- Middle Name;
- DOB;
- SSN; and
- Gender.

The sharing of this data is internal to USSS personnel specifically granted access to perform these queries. Employees using those systems must contact PID directly for more detailed information about a subject/case in PTMS. This ensures the most detailed information is shared with only people with a need to know.

Uses of the Information

The usage of the PTMS data has changed. Two additional uses have been implemented. USSS leverages the data within PTMS for background investigations for both individuals in the hiring process and NSSE attendees.

Notice

The DHS/USSS-004 Protection Information System System of Records Notice (SORN)[5] provides notice regarding the collection of information and the routine uses associated with the collection the information. Notice to individuals prior to collection of information is not feasible in that it could impede law enforcement investigation.

Data Retention by the project

There are no changes to the data retention schedule for this system.

Information Sharing

PTMS internal sharing has changed. There are new interconnections between the USSS ALIS and eCheck systems. ALIS and eCheck query the PTMS database schema to determine if a USSS job applicant has an open case or a NSSE attendee is a person of interest identified by PID.

The sharing of this data is internal to USSS personnel specifically granted access to perform these queries. Employees using those systems must contact PID directly for more detailed

[5] DHS/USSS-004 Protection Information System, 76 FR 66940 (October 28, 2011).

information about a subject/case in PTMS. This ensures the most detailed information is shared with only people with a need to know.

PII and/or summary investigative information maintained in PTMS may be shared with federal, state, and local law enforcement agencies, other foreign and domestic government units, and with private entities on a need-to-know basis to further investigations and assignments by the Secret Service. The Secret Service transmits information in a variety of ways, including electronically, in oral briefings, interviews, in writing, or by telephone. Only Secret Service employees who need the information to effectively perform their job functions can gain access to PTMS.

PTMS information is shared with law enforcement and other U.S. Government agencies with a protective mission or other federal/state/local government, foreign government units, and health officials who, by their jurisdictional responsibilities, have a need-to-know. This external sharing is compatible with the original law enforcement collection and is consistent with the routine uses contained in the DHS/USSS-004 Protection Information System SORN.

To the extent that information may be released pursuant to any other routine uses, such release may only be made if it is compatible with the purposes of the original collection, as determined on a case-by-case basis.

Privacy Risk: There is a risk of improperly disclosing PII outside of the Department.

Mitigation: This risk is mitigated by integrating administrative, technical, and physical security controls that protect PII against unauthorized disclosure. Disclosure may only be made by authorized Secret Service employees engaged in protective activities who are trained on the use of PTMS. Authorized Secret Service users of PTMS may only share the data with recipients listed in the SORN who have a need-to-know.

Redress

As a protection information system owned by the Secret Service, the DHS/USSS-004 Protection Information System SORN contains exemptions from the access and redress provisions of the Privacy Act. However, access requests will be considered on a case-by-case basis if made in writing to the Secret Service's Freedom of Information Act (FOIA) Officer, Communications Center (FOIA/PA), 245 Murray Lane, Building T-5, Washington, D.C. 20223, as specified in the SORN.

Privacy Risk: There is a risk that that an individual may have limited access or ability to correct their information.

Mitigation: Individuals can request access to information about themselves under the FOIA and Privacy Act and may also request that their information be corrected. The nature of PTMS and the information it collects and maintains is such that the ability of individuals to access or correct their information may be limited by Privacy Act exemptions. The redress and access

measures offered are appropriate given the purpose of the system, which is to collect, analyze, and store information concerning individuals who may pose a threat to Secret Service protectees, protected facilities, and protected events. However, requests to amend records will be considered on a case-by-case basis if made in writing to the Secret Service's FOIA Officer, Communications Center (FOIA/PA), 245 Murray Lane, S.W., Building T-5, Washington, D.C. 20223.

Auditing and Accountability

All Secret Service information systems are audited regularly to ensure appropriate use of and access to information. Specifically related to this system, application access is mediated through a two-tier identification and authentication process. Any changes to the hardware or software configuration are subject to review and approval by the USSS Configuration Control Board process to ensure integrity of the application

All Secret Service employees and contractors are required to receive annual privacy and security training to ensure their understanding of proper handling and securing of PII. Also, DHS has published the "Handbook for Safeguarding Sensitive PII," providing employees and contractors additional guidance.

DHS physical and information security policies dictate who may access USSS computers and filing systems. Specifically, DHS Sensitive Systems Policy Directive 4300A outlines information technology procedures for granting access to Secret Service computers. Access to the system is strictly limited to authorized Secret Service employees who have a need to know in the furtherance of their role in protective intelligence analysis. User access to the PTMS is controlled by role-based permissions and includes various levels depending on the user's function in the USSS.

Responsible Official

Fred Sellers
Assistant Director - Strategic Intelligence and Information
U.S. Secret Service

Approval Signature

[Original signed and on file with the DHS Privacy Office]

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