Privacy Impact Assessment
for the

Protective Threat Management System (PTMS)

DHS/USSS/PIA-003

August 25, 2016

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 replaces the Protective Research Information Management System (PRISM-ID) and the Counter Surveillance Unit Reporting (CSUR) database, which had both exceeded their useful lifecyle and were costly to update and maintain. The Secret Service is conducting this Privacy Impact Assessment (PIA) because PTMS collects personally identifiable information (PII), replaces PRISM-ID and CSUR, and has a new proposed retention schedule. The previously published PIAs for PRISM-ID and CSUR will be retired upon publication of this PIA.

Overview

The United States Secret Service (Secret Service or USSS) Protective Threat Management System (PTMS) is a case management system used to record information that is required to assist the agency in meeting its protective mission that 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 record PII information 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 and/or 879, or other appropriate federal/state statute. 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 replaces PRISM-ID, and the separate CSUR Database, which had exceeded their useful lifecycle and were costly to update and maintain. PRISM-ID was the case management system used to maintain information on individuals expressing threatening or inappropriate behavior and a variety of other incidents related to the Secret Service's protective mission describe above. CSUR was the case management system used to record data on suspicious behavior reported near Secret Service protected sites or facilities. Data from PRISM-ID and CSUR was either migrated to PTMS or purged according to provisions of the corresponding legacy records control schedules. All of the functionality of PRISM-ID and CSUR were replicated in PTMS.

PTMS includes features such as workflow record keeping, new data fields to reflect changing requirements, the ability to attach electronic documents, more accurate 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 initated by the Secret Service, but may also contain case records that contain information received from other government agencies 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 movement or protected event.[1]

Access to the PTMS is strictly limited to authorized Secret Service employees who have a legitimate need to know in the furtherance of their role in protective intelligence analysis. User access to the PTMS is controlled by Active Directory and includes various levels depending on the user’s function in the USSS. The most restrictive 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 the PTMS (e.g., case agent name, an arrest date, or case disposition). Staff assigned to the Protective Intelligence and Assessment Division at USSS headquarters are granted additional access, allowing these users to create and edit report/case records. The least restrictive level of access is granted to certain supervisors in the Protective Intelligence and Assessment Division who may retire or purge entire case records, edit the pre-populated values available for users to select in list-of-value fields in the 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.

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, 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

[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.”

familiar with the subject. PTMS does not perform biometric analysis.

Headquarters users in the Protective Intelligence and Assessment Division (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 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 little or no system rights to edit records. These users are also restricted to viewing only portions of records 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 when records were created or updated. PTMS does not connect to external systems. PTMS records are not automatically updated and cannot be manually updated without an authorized user accessing PTMS.

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, 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 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 protectee 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, 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.

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 Secret Service is authorized to collect information maintained in PTMS pursuant to 18 U.S.C. §§ 3056 and 3056A.

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

The DHS/USSS-004 Protection Information System[2] applies to the collection, use, maintenance, and dissemination of PII by PTMS.

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

No. The Authority to Operate for PTMS is pending completion of this PIA.

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

The Secret Service retains the information no longer than is useful or appropriate for carrying out the information dissemination, collaboration, or investigation purposes for which it was originally collected. Information collected that becomes part of a case is retained in PTMS for a period that corresponds to the specific case disposition assigned.

As documented in a corresponding DHS Investigative Records Disposition Schedule,[3] the

[2] DHS/USSS-004 Protection Information Systems SORN, 76 FR 66940 (October 28, 2011), *available at* http://www.gpo.gov/fdsys/pkg/FR-2011-10-28/html/2011-27883.htm.

[3] DHS Investigative Records Disposition Schedule (currently pending National Archives and Records Administration (NARA) endorsement).

disposition for PTMS records (comprising records of threats, unusual behavior, and background information pertaining to persons, incidents, groups of interest, and trips or events) are retained for 30 years following the end of the investigation.

The proposed retention schedule has been endorsed by the Secret Service Chief Records Officer and has been forwarded for inclusion in the DHS Investigative Records Disposition Schedule. Pending NARA approval of the Enterprise schedule, records produced by the system are retained and disposed of in a manner consistent with the proposed draft, in accordance with 36 CFR 1226.18 ("Agencies may retain records eligible for destruction until the new schedule is approved.").

As reflected in both current and pending schedules, the disposition for records of threats, unusual behavior, and background information pertaining to persons, incidents, groups of interest, and trips or events reflect a 30 year retention. Certain incidents of significant historical interest (e.g., assassination attempts, successful assassinations) are designated for permanent retention and transfer to NARA under records retention schedule N1-87-89-1.[4]

With this updated records retention schedule, USSS will update the DHS/USSS-004 Protective Information System[5] SORN to reflect the newly published retention requirements.

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.

Due to the law enforcement nature of this information collection, the information collected in PTMS is not covered by the Paperwork Reduction Act.

Section 2.0 Characterization of the Information

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

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

PTMS maintains PII and biographical information for subjects when the Secret Service requires such information to perform its protective responsibilities. PTMS may maintain the

[4] Records retention schedule N1-87-89-1 *available at* http://www.archives.gov/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0087/n1-087-89-001_sf115.pdf.

[5] DHS/USSS-004 Protection Information Systems SORN, 76 FR 66940 (October 28, 2011), *available at* http://www.gpo.gov/fdsys/pkg/FR-2011-10-28/html/2011-27883.htm.

following types of PII, including:

Information regarding subjects, including:

- Name and/or Alias;
- Images of known and unknown subjects;
- Images of evidence containing PII (e.g., an envelope with return address);
- Images of vehicles;
- Address;
- Email Address;
- Internet Protocol (IP) Address;
- Date and/or Place of Birth;
- Race and Sex;
- Social Security number;
- Driver's License/State ID Number;
- Passport Number;
- Alien Registration Number;
- Federal Bureau of Investigation (FBI) and/or State Criminal Record Identification Number;
- Prisoner Number;
- Identification Numbers issued by other foreign or domestic government units; and/or
- Case Number.

Information regarding protected persons, trips, and events, including:

- Date(s) of a trip or event;
- Location of a trip or event; and
- Name of the protected person or event.

Information regarding incidents (incidents are specific occurrences in which the Secret Service has an interest) including:

- Date(s) of an incident;

- Location of an incident:
- Name of the incident; and
- Description of the incident.

An incident is the occurrence of an event or activity that may be of protective interest to the Secret Service. Incidents usually involve one or more of the following: a criminal or violent act committed by a subject of record with the Secret Service; an act committed by an individual or organization employing methods of subversion, terrorism, or sabotage; an act or behavior directed toward a public figure, public official, or Government entity; and/or any event that could be detrimental to the Secret Service protective mission.

PTMS maintains other administrative case information including:

- Employees assigned;
- Source of information, specifically: direct contact, law enforcement/corrections, intelligence community agency, other government agency, foreign government, hospital/mental health facility, concerned citizen, USSS, USSS-Countersurveillance Division, or Open Source;
- Dates of investigation, if any;
- Dates of approval, when required;
- Office(s) assigned;
- Other Secret Service offices or agencies for which information was shared about the case or subject;
- Whether a subject was submitted to the National Instant Background Check System (NICS);
- Whether a subject was reviewed by the Secret Service National Threat Assessment Center;
- Dates a subject was interviewed by a Secret Service special agent;
- Requests made by headquarters to field offices; and
- Indications of whether or not:
    - the case was responsive to a Freedom of Information Act request;
    - the case was responsive to a legal proceeding involving the Secret Service;
    - a physical file exists; or
    - the case was used as part of a Secret Service study.

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

Sources of information for PTMS include:

- U.S. Government agencies to include, but not limited to, the Executive Office of the President, Departments (and various component agencies) of Homeland Security, Justice, Defense, Interior, Treasury, Health and Human Services, U.S. Capitol Police, U.S. Supreme Court Police, and Intelligence Community agencies[6] provide the Secret Service with information relevant to protectee travel and potential threats to Secret Service protectees or protected events.
- Foreign government agencies may provide the Secret Service with information pertaining to potential threats to Secret Service protectees.
- Law enforcement agencies provide the Secret Service with information
- Open source information, to include media and individual reports over broadcast and internet/social media, may be used to corroborate information or identify investigative leads.
- Public records, available through subscription or publically available internet sites, may be used to corroborate information or identify investigative leads.
- Concerned citizens may make reports to the Secret Service or other agencies relevant to potential threats to Secret Service protectees or protected events.
- Secret Service personnel, in the course of their official duties, may serve as the source of information concerning potential threats to Secret Service protectees and protected events.

The information may be received via official report, queries of government and public record systems, Internet searches, unsolicited emails or telephone calls, or in-person meetings. Queries of government and public record systems most often include, but are not limited to, the National Crime Information Center; National Law Enforcement Telecommunications System; Targeted Violence Information Sharing System;[7] U.S. Bureau of Prisons and state inmate locator systems; eGuardian (FBI);[8] Intelligence Community records shared with the Secret Service; and various public records available.

Information is collected directly from the individual, through investigations and/or liaison

[6] See https://www.dni.gov/index.php/intelligence-community/members-of-the-ic.

[7] DHS/USSS/PIA-002 Targeted Violence Information Sharing System (TAVISS), *available at* www.dhs.gov/privacy.

[8] *See* FBI eGuardian PIA, *available at* https://www.fbi.gov/services/records-management/foia/privacy-impact-assessments/eguardian-threat.

activities conducted by Secret Service personnel, or is provided to the Secret Service unsolicited. Secret Service personnel who are authorized and have access may enter the collected information directly into PTMS to update or complete a record. Users may also attach an electronic copy of the source record to the PTMS case record.

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

USSS routinely collects publicly available information, to include social media, and information that may be obtained through commercially available Internet sources. USSS uses such tools for situational awareness regarding protected persons, events, or facilities, and to ascertain the location of subjects of investigations. This information may be used to develop preliminary leads.

2.4 Discuss how accuracy of the data is ensured.

The information is checked for accuracy during the course of the investigative process through personal interviews and again when information is entered into PTMS, when discrepancies may be detected. Typically, discrepancies are due to data entry errors. If discrepancies are found, protective intelligence personnel can correct the entry and update the information.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: Due to the inherent risk of inaccurate information from publicly available sources, such as social media, there is a risk that the Secret Service will incorrectly identify individuals as the subjects of protective threat assessments.

Mitigation: This risk is partially mitigated. Secret Service identifies information from third-party social media services submitted voluntarily by members of the public and compares that information with information available through a variety of public and government sources. By bringing together and comparing many different sources of information, Secret Service personnel attempt to provide a more accurate picture of potentially threatening activities. Requests to amend records will be considered on a case-by-case basis if made in writing to the Secret Service's FOIA/PA Officer, Communications Center (FOIA/PA), 245 Murray Lane, S.W., Building T-5, Washington, D.C. 20223.

Privacy Risk: There is a risk of over collection of information when the Secret Service collects publicly available information associated with a particular location or event to be visited/attended by a Secret Service protectee or otherwise secured by the Secret Service.

Mitigation: Data is most often collected by the Secret Service from other law enforcement agencies or directly from the individual during the course of an investigation based on voluntary cooperation. Data may also be obtained lawfully from public or law enforcement records (e.g., existing PTMS or other agency records). Further, the Secret Services uses PII for the limited purpose of enabling positive identification so that (a) the individual is identifiable during future interactions with the agency; (b) the individual is not erroneously identified as, or linked to, another individual; and (c) further investigation can be conducted, if necessary.

Privacy Risk: There is a risk of inaccurate information because PTMS relies heavily on information from other government law enforcement databases and is generally not the original source of collection.

Mitigation: No action will be taken unless the information received has been reviewed by Secret Service employees engaged in protective activities who are trained in the interpretation of the information and familiar with the environment in which the information is collected and used. PTMS supports USSS personnel in identifying individuals known to the Secret Service or other U.S. Government agencies who may pose a risk of harm to protected persons, events, or facilities.

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.

The information is used to support the Secret Service in accomplishing its protective mission, specifically in development of threat assessments to assist 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. The Secret Service uses PTMS to identify individuals known to the Secret Service or other U.S. Government agencies who may pose a risk of harm to protected persons, events, or facilities.

Data is collected in order to assess an individual, group, or incident that may pose a threat or potential threat to Secret Service protected persons, events, or facilities. The results of such investigations and/or assessments are disseminated to internal Secret Service customers, including protective details, to support their protective efforts, and within the Department of Homeland Security.

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.

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

No.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: The privacy risks associated with the uses of information are possible misuse and inappropriate dissemination of PII records.

Mitigation: To mitigate these risks, the Secret Service uses this information for the limited purpose of developing preliminary leads that are subsequently investigated by special agents through personal interviews in order to identify subjects of investigation or their possible whereabouts. Access to the system is limited to authorized Secret Service employees who have a need to know in the furtherance of their role in protective intelligence analysis.

All Secret Service employees and contractors are required to follow DHS Management Directive (MD) Number: 11042.1– Safeguarding Sensitive But Unclassified (For Official Use Only) Information. This guidance controls the manner in which employees and contractors must handle Sensitive but Unclassified/For Official Use Only Information. All employees and contractors are required to follow Rules of Behavior contained in the DHS Sensitive Systems Policy Directive 4300A, March 14, 2011. Additionally, all Secret Service employees are required to take annual computer security and privacy training, which includes training on the appropriate use and handling of sensitive data and proper security measures.

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 DHS/USSS-004 Protection Information System SORN 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. The final rule for the system of records officially exempts the system from portions of the Privacy Act.[9]

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

None. Due to the law enforcement nature of this information collection, individuals do not have the right to consent to particular uses of the information in PTMS.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals will not have notice that their information has been collected by the Secret Service and stored in PTMS due to the law enforcement nature of the collection.

Mitigation: This risk cannot be mitigated. It is not possible to provide notice to individuals prior to the collection of information as such notice could impede law enforcement investigations because the purpose of PTMS is to assist USSS protective operations personnel in identifying individuals known to the Secret Service or other U.S. Government agencies who may pose a risk of harm to protected persons, events, or facilities. However, this PIA and the USSS Protection Information System SORN serve as public notice of the existence of PTMS, the data it collects and maintains, and the routine uses associated with the information collected.

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.

All collected information that is entered in PTMS, as outlined in Section 2 is retained as set out in Section 1.4 above. Such information may include specific information about an action or incident that brought an individual to Secret Service attention, PII on the subject of an investigation or other individuals related to the investigation, and other personal history of the individual investigated.

The Secret Service retains the information no longer than is useful or appropriate for carrying out the information dissemination, collaboration, or investigatory purposes for which it was originally collected. Information collected that becomes part of a case is retained in PTMS for a period that corresponds to the specific case disposition assigned.

[9] 74 FR 45090, August 31, 2009.

As documented in a corresponding DHS Investigative Records Disposition Schedule[10], the disposition for the system's Master File (comprising records of threats, unusual behavior, and background information pertaining to persons, incidents, groups of interest, and trips or events) reflect a 30 year retention.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a privacy risk that information will be retained for longer than necessary to accomplish the purpose for which the information was originally collected.

Mitigation: The information in PTMS will be retained for the timeframes outlined in section 5.1 to allow the Secret Service to manage, analyze, and distribute intelligence information regarding threats or potential threats to the safety of individuals, events, and facilities protected by the Secret Service. The retention period is also consistent with the general law enforcement system retention schedules currently being adjudicated by DHS/NARA, and is appropriate given the Secret Service protective mission and the importance of the law enforcement data to accomplish this mission.

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.

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.

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

PTMS information is shared with law enforcement and other U.S. Government agencies

[10] DHS Enterprise Records Disposition Schedule (currently pending National Archives and Records Administration (NARA) endorsement).

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.

The Secret Service may share personally identifiable information and/or summary investigative information with external partners. 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.

6.3 Does the project place limitations on re-dissemination?

Information maintained in PTMS is shared with recipients listed in the applicable SORN (DHS/USSS-004 Protection Information Systems) who have a need-to-know in the performance of their official duties. Security warnings and disclaimers requiring that the information be kept in law enforcement channels are orally reinforced during telephone calls. The USSS routinely marks its intelligence documents as “not for further dissemination without permission.”

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

When PTMS information is shared with outside law enforcement organizations, and/or other federal, state, local government agencies, an entry is made in PTMS to reflect that the information was shared and with whom it was shared. Most disclosures are recorded on a form (see Figure 6.4).

At other times, disclosures may be noted at the end of a record by manually typing information to identify the date and receiving agency. Disclosures may also be recorded by attaching the disclosed information to the source record in PTMS.

6.5 Privacy Impact Analysis: Related to Information Sharing

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.

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?

As a protection information system owned by the Secret Service, the DHS/USSS-004 Protection Information System SORN permits PTMS to be excluded 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.

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

The procedures are the same as those outlined in Question 7.1.

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

The mechanism for requesting correction of information contained in any Secret Service protection information system is specified in the DHS/USSS-004 Protection Information System SORN, and also available on the Secret Service's public webpage.

7.4 Privacy Impact Analysis: Related to Redress

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/PA Officer, Communications Center (FOIA/PA), 245 Murray Lane, S.W., Building T-5, Washington, D.C. 20223.

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?

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.

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

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.

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

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 legitimate need to know in the furtherance of their role in protective intelligence analysis. User access to the PTMS is controlled by Active Directory and includes various levels depending on the user's function in the USSS. The most restrictive level of access is granted to special agents (who investigate individuals expressing threatening or inappropriate behavior and other incidents that may impact the Secret Service's mission to protect persons, events, and facilities) and field-based administrative personnel who record administrative case information in the PTMS (e.g., case agent name, an arrest date, or case disposition). Staff assigned to the Protective Intelligence and Assessment Division at USSS headquarters are granted additional access, allowing those users to create and edit report/case records. The least restrictive level of access is granted to certain supervisors in the Protective Intelligence and Assessment Division who may retire or purge entire case records, edit the pre-populated values available for users to select in list-of-value fields in the 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.

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?

All information sharing agreements, MOUs, and new uses of information are reviewed by the USSS Privacy Office, Office of Chief Counsel, and the respective program office.

Responsible Officials

J. Mark Bartlett
Assistant Director - Strategic Intelligence and Information
U.S. Secret Service

Latita Payne
Privacy Officer
U.S. Secret Service

Approval Signature

Original copy on file with DHS Privacy Office.

____

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