



Privacy Impact Assessment Update
for the

PRISM-ID

November 10, 2010

Contact Point

Latita Payne

Disclosure Officer

U. S. Secret Service

202-406-5838

Reviewing Official

Mary Ellen Callahan

Chief Privacy Officer

Department of Homeland Security

(703) 235-0780



Abstract

The United States Secret Service (Secret Service) has created and uses the Protective Research Information System Management (PRISM-ID) system to record information that in accordance with Secret Service criteria 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 First Ladies, major candidates for the presidency and vice presidency, foreign heads of state visiting the United States, and other individuals authorized to receive Secret Service protection. This PIA is being conducted because PRISM-ID collects personally identifiable information (PII).

Overview

The PRISM-ID system records data on threats, inappropriate or unusual behavior, and incidents that may impact the Secret Service's mission to protect persons, events, and facilities. The system also may contain PII on subjects of an investigation. PRISM-ID does not include information on individuals merely seeking access to protected facilities or sites unless they are the subject of an investigation or otherwise came to the attention of the Secret Service for threatening, inappropriate, or unusual behavior. Information may include 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.

Information from PRISM-ID is used to develop threat assessments to assist protective operations in creating a secure environment for Secret Service protected persons, events, and facilities. Use of the PRISM-ID system is restricted to personnel who need information to effectively perform their job functions.

Types of personally identifiable information (PII) that may be maintained in PRISM-ID include:

- Name and/or Alias;
- Address;
- E-mail Address;
- Date and/or Place of Birth;
- Social Security Number;
- Driver's License/State ID Number;
- Passport Number;
- Alien Registration Number;
- FBI and/or State Criminal Record Identification Number;
- Prisoner Number;
- Identification Numbers issued by other foreign or domestic government units; and/or
- Case Number.

Authorized headquarters users of PRISM-ID enter data into the system through use of a computer interface. Queries for information may be conducted 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. Queries of the PRISM-ID system are used to:



- Develop threat assessments for protected persons by identifying cases of interest;
- 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 the Department of Homeland Security, Office of Management and Budget, and the U.S. Congress.

An example of a typical transaction would be an authorized user entering information into PRISM-ID to reflect the office assigned an investigation or a text summary of an incident. Examples of typical queries would be an authorized user entering query criteria to identify a subject by name; or to report how many cases were investigated in a particular city; or to identify how many subjects were arrested for violation of federal law in a given time period.

The Secret Service is authorized to collect information maintained in PRISM-ID pursuant to Title 18 U.S.C. §§ 3056 and 3056A.

Section 1.0 Characterization of the Information

1.1 What information is collected, used, disseminated, or maintained in the system?

PRISM maintains PII and life history information of individuals where such information is required by the Secret Service in the performance of its protective responsibilities. Types of PII that may be maintained in PRISM-ID include:

- Name and/or Alias;
- Address;
- E-mail Address;
- Date and/or Place of Birth;
- Social Security Number;
- Driver's License/State ID Number;
- Passport Number;
- Alien Registration Number;
- 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 person trips and events, such as time, place, and incidents occurring during the trip or event, and other administrative case information are also maintained in PRISM-ID.

1.2 What are the sources of the information in the system?



U.S. Government agencies, foreign government agencies, federal, state, and local law enforcement, the media, public records, concerned citizens, and Secret Service personnel may serve as sources of information for PRISM-ID. The information may be received via official report, queries of government and public record systems, unsolicited e-mails or telephone calls, or in-person meetings.

1.3 Why is the information being collected, used, disseminated, or maintained?

The information is required in support of the Secret Service protective mission. 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.

1.4 How is the information being collected?

Information is collected through investigations and/or liaison activities conducted by Secret Service personnel or is provided to the Secret Service unsolicited. Secret Service personnel who are authorized and have access to the system enter the information directly into PRISM-ID.

1.5 How will the information be checked for accuracy?

The information is checked for accuracy during the course of the investigative process and again when information is entered into the PRISM-ID system, when discrepancies may be detected.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

The collection of the information is authorized by the Secret Service's protective authority contained in 18 U.S.C. §§ 3056 and 3056A.

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

Privacy risks associated with PRISM-ID concern erroneous entry of an individual's PII into PRISM-ID. However, the risk is minimal because data is most often collected by Secret Service or other law enforcement officers 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 PRISM-ID or other agency records). Further, any adverse impact on individuals is mitigated because the Secret Service limits access to the data. Further, PII information is used 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).



Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe the uses of 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. The system supports this by enabling the Secret Service to identify individuals known to the Secret Service or other U.S. Government agency that may pose a risk of harm to protected persons, events, or facilities.

2.2 What types of tools are used to analyze data and what type of data may be produced?

The PRISM-ID system has built-in search functionality that may produce case information by case number, administrative information such as case assignments, controlling office, personally identifiable information, and other data elements extracted from the system.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

USSS collects information in the course of an investigation that may be obtained through commercially available sources such as LexisNexis Law Enforcement Solutions®. USSS uses such solutions to ascertain the location of subjects of investigations or persons of interest through public and proprietary LexisNexis databases. This information is used to develop preliminary leads that are subsequently investigated by special agents through personal interviews in order to verify accuracy of information. USSS is responsible for ensuring that public or commercial data is accurate to the extent possible before inputting it into PRISM.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

The privacy risks associated with the uses of information are possible misuse and inappropriate dissemination of PII and the use of commercial data for a purpose other than the purpose for which it was collected. To mitigate these risks, this information is used 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.

To further mitigate these risks, the Secret Service has implemented the following security measures:



1. Identification/Authentication – establishes user accountability and validity of identification;
2. Auditing – records user activity for after the fact investigation of all transactions;
3. Accountability – enables security-relevant activities on a system to be traced to individuals who may then be held responsible for their actions;
4. Access Control – access is limited only to authorized programs and/or systems. Also, only users who need the information to effectively perform their job functions can gain access to PRISM-ID using a PRISM-ID user and password to view the data;
5. Confidentiality – assures that information is not made available or disclosed to unauthorized individuals, entities, or processes;
6. Integrity – assures that information has not been altered or destroyed in an unauthorized manner; PRISM-ID login includes a security warning to users concerning the appropriate use of the system's data.

All Secret Service employees and contractors are trained on the appropriate use of PII as well. Access to PRISM-ID is also limited to Secret Service employees who need access to effectively perform their jobs.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

All collected information that is entered in PRISM-ID, as outlined in Section 1.1, is retained. 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 are retained.

3.2 How long is information retained?

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 which is collected that becomes part of a protective intelligence case is retained in PRISM-ID for a period which corresponds to the specific case type developed.

As submitted to NARA, 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) reflects a 20 year retention.

3.3 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

Investigative records produced by the system are retained and disposed of in accordance with various disposition schedules approved by the Secret Service Chief Records Officer and the National Archives and Records Administration. Consistent with requirements contained within 36



CFR § 1234, efforts to schedule PRISM-ID as a distinct electronic system are ongoing and final approval is anticipated in the near future.

As submitted to NARA, 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) reflects a twenty year retention.

3.4 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

Risks associated with data retention are mitigated by restricting access to the information in PRISM-ID. Only Secret Service employees requiring access to PRISM-ID to complete their work functions are allowed access to the system. Also, specific searches, based upon when a record was established, are performed on a recurring basis to determine files requiring deletion.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

PRISM-ID information is shared within the Secret Service and DHS departmental offices and component agencies to the extent required to enable authorized officials to complete their functions and responsibilities. Authorized officials may include those with a need-to-know PRISM-ID information so that they may provide effective protection of persons, events, or facilities; investigate potential criminal activity; or ensure the protection of National Security Information.

4.2 How is the information transmitted or disclosed?

PRISM-ID information is shared via in-person or telephonic contact, fax, or email.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Privacy risks associated with internal sharing of the data is unauthorized access to, or disclosure of, PII contained in PRISM-ID. To mitigate this risk, access to the system is limited to only Secret Service employees with a need-to-know. DHS policies and procedures are in place to limit the use of and access to all data in PRISM-ID to the purposes for which it was collected. All authorized users must log on using a two-factor authentication. Computer security concerns are minimized by the fact that the information shared internally remains within the DHS environment. An audit trail is kept for system access and all transactions that request, create, update, or delete information from the system. The audit trail/log, which includes the date, time, and user for each transaction, is secured from unauthorized modification, access, or destruction.



All DHS employees and contractors are required to follow DHS Management Directive (MD) Number: 11042, *Safeguarding Sensitive But Unclassified (For Official Use Only) Information*, May 11, 2004. This guidance controls the manner in which DHS 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 Handbook. Additionally, all DHS employees are required to take annual computer security training, which includes training on appropriate use of sensitive data and proper security measures.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS which included Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared and for what purpose?

Personally identifiable information and/or summary investigative information maintained in PRISM-ID 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 support protective investigations and assignments by the Secret Service. However, any information maintained in PRISM-ID may be shared in accordance with the purposes and routine uses specified in the Secret Service's System of Records Notice DHS/USSS-004 (Protection Information System, 73 FR 77733) in support of the Secret Service protective mission.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

The sharing of PII data outside the Department is compatible with the original collection and is consistent with the routine uses contained in the Secret Service's System of Records Notice DHS/USSS-004 (Protection Information System, 73 FR 77733). PRISM-ID information is shared with law enforcement and other U.S. Government agencies with a protective mission or other federal/state/local government or health officials who, by their jurisdictional responsibilities, have a need-to-know. Personally identifiable information and/or summary investigative information may be shared. 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.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

Secret Service transmits information in a variety of ways, including electronically, in oral



briefings, and interviews, in writing, or by telephone. The method of transmission depends on the nature and sensitivity of the information, privacy interests, status of the investigation, and/or confidentiality.

Only Secret Service employees who need the information to effectively perform their job functions can gain access to PRISM-ID. Any information shared by Secret Service employees with organizations outside the Secret Service is required to be appropriately secured pursuant to the Office of Management and Budget Memorandums 06-15, Safeguarding Personally Identifiable Information, and 06-16, Protection of Sensitive Agency Information.

Secret Service developed and implemented PRISM-ID in accordance with approved security guidelines.

5.4 Privacy Impact Analysis: Considering the external sharing, explain the privacy risks identified and how they were mitigated?

The privacy risk identified is the disclosure of personally identifiable information to an unauthorized recipient. To mitigate this risk, disclosure may only be made by authorized Secret Service employees engaged in protective activities who are trained on the use of PRISM-ID. Authorized Secret Service users of PRISM-ID may only share the data with law enforcement and other U.S. Government agencies with a protective mission or other federal/state/local government or health officials who, by their jurisdictional responsibilities, have a need-to-know.

Section 6.0 Notice

6.1 Was notice provided to the individual prior to collection of information?

The System of Records Notice DHS/USSS-004 (Protection Information System, 73 FR 77733) 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.

6.2 Do individuals have the opportunity and/or right to decline to provide information?

Individuals have no right to decline to have their information collected, stored, and maintained in this system.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

Individuals do not have the right to consent to particular uses of the information maintained in PRISM-ID.



6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

The System of Records Notice DHS/USSS-004 (Protection Information System of Records Notice, 73 FR 77733) provides notice regarding the collection of information, and the routine uses associated with the collection the information. Risks are mitigated through verification and validation during the course of the investigative process and again when information is entered into the PRISM-ID system, when discrepancies may be detected.

Section 7.0 Access, Redress and Correction

7.1 What are the procedures that allow individuals to gain access to their information?

As a protection information system owned by the Secret Service, System of Records Notice DHS/USSS-004 (Protection Information System of Records Notice, 73 FR 77733) permits PRISM-ID 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 FOIA Officer, Communications Center (FOIA/PA), 245 Murray Lane, Building T-5, Washington DC 20223, as specified in the Systems of Records Notice.

7.2 What are the procedures for correcting inaccurate or erroneous information?

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

7.3 How are individuals notified of 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 System of Records Notice DHS/USSS-004 (Protection Information System of Records Notice, published in the Federal Register at 73 FR 77733) and also available on the Secret Service's public webpage.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Although redress may not be available through the Secret Service because PRISM-ID is an exempt system of records and not subject to the redress requirements, an individual may submit a letter to the Secret Service Freedom of Information Officer addressing his or her concerns.



7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated?

Redress is available through written request to the Secret Service Freedom of Information Officer as described above; however, providing individual access and/or correction of the records may be limited for law enforcement reasons as expressly permitted by the Privacy Act. Risks are also mitigated because PRISM-ID data is never used directly as evidence to prosecute crimes.

Section 8.0 Technical Access and Security

8.1 What procedures are in place to determine which users may access the system and are they documented?

DHS physical and information security policies dictate who may access USSS computers and filing systems. Specifically, DHS Management Directive 4300A outlines information technology procedures for granting access to Secret Service computers. Access to the information is strictly limited by access controls to those who require it for completion of their official duties.

8.2 Will Department contractors have access to the system?

All Secret Service users of the PRISM-ID system are Secret Service employees. Contractors have not been given access to this system.

8.3 Describe what privacy training is provided to users to either generally or specifically relevant to the program or system?

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.

8.4 Has Certification and Accreditation been completed for the system of systems supporting the program?

The system has undergone certification and accreditation.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

All Secret Service information systems are audited regularly to ensure appropriate use and access to information. In addition, several of the tables have audit tables populated by triggers that capture all additions, modifications and deletions of main case data. There are also technical



safeguards such as the use of client software which is installed on work stations and requires a valid approved user identification and password.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

As a protection information system owned by the Secret Service, PRISM-ID is covered by the System of Records Notice DHS/USSS-004 (Protection Information Systems, 73 FR 777333) which specifies how the information may be used. Also, all Secret Service employees and contractors are trained on the appropriate use of PII.

In addition, seven primary security standards were established for PRISM-ID. These include:

1. Identification/Authentication – establishes user accountability and validity of identification;
2. Auditing – records user activity for after the fact investigation of all transactions;
3. Accountability – enables security-relevant activities on a system to be traced to individuals who may then be held responsible for their actions;
4. Availability – assures that data is in the place where the user needs it, when the user needs it, and in the proper form;
5. Access Control – limits access only to authorized programs and/or systems;
6. Only the limited work stations with the PRISM-ID client, a user and password can view the data;
7. Confidentiality – assures that information is not made available or disclosed to unauthorized individuals, entities, or processes; and
8. Integrity – assures that information has not been altered or destroyed in an unauthorized manner; PRISM-ID login includes a security warning to users concerning the appropriate use of the system's data.

Section 9.0 Technology

9.1 What type of project is the program or system?

PRISM-ID is comprised of standard commercial hardware and software which has been modified to meet the need of the Secret Service.

9.2 What stage of development is the system in and what project development lifecycle was used?

The system is in the operations and maintenance lifecycle phase.



9.3 Does the project employ technology which may raise concerns? If so please discuss their implementation.

The project does not employ technology which may raise privacy concerns.

Responsible Official

Latita Payne
United States Secret Service
Department of Homeland Security
Communications Center (LIA: 3000)

245 Murray Lane SW, Bldg T-5
Washington, DC 20223
Office: 202-406-5838

Approval Signature

Original signed and on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security