PRIVACY IMPACT ASSESSMENT (PIA) 3-YEAR REVIEW COVER PAGE

Component: *United States Secret Service*

Name of Program/System: *Targeted Violence Information Sharing System (TAVISS)*

This system has undergone a PIA 3-Year Review on: *August 19, 2013*

The DHS Privacy Office works with DHS components to ensure that PIA reviews are conducted every three years.

DHS requires each component PIA to be reviewed in conjunction with the expiration of the accompanying PTA, in an effort to determine whether significant changes have been made to the system. This review ensures that each system continues to accurately relate to its stated mission.

Specifically, the PIA 3-Year Review Adjudication addresses each of the main areas of the PIA relating to: Legal Authorities; Characterization of the Information; Uses of the Information; Notice; Data Retention; Information Sharing; Redress; and Auditing and Accountability.

The above mentioned PIA has had no changes to the privacy risks and mitigations identified in the published PIA. The information technology certification and accreditation (C&A) approval has been extended to August, 2016.

Privacy Impact Assessment
for the

Targeted Violence Information Sharing System (TAVISS)

July 13, 2010

DHS/USSS/PIA-002

Contact Point
Latita Payne
U. S. Secret Service
(202) 406-5503

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 the Targeted Violence Information Sharing System (TAVISS). TAVISS is used to conduct name checks and determine whether a subject is of protective interest to any agency within the TAVISS network. The Secret Service is conducting this Privacy Impact Assessment (PIA) because TAVISS contains personally identifiable information (PII) regarding subjects of protective interest to the Secret Service and participating agencies in the network.

Overview

The Protective Intelligence and Assessment Division of the Secret Service uses TAVISS, a shared system directly accessed from remote sites by multiple law enforcement agencies with protective responsibilities for public officials. All TAVISS users are members of a law enforcement agency engaged in protection pursuant to that agency's specific authorizing federal or state legislation and the rules and regulations applicable to law enforcement agencies.

The system enables participating agencies to conduct name checks and determine whether a subject is of record with any agency within the TAVISS network. All queries limit search criteria to a subject's personal identifiers (i.e., name, sex, race, date of birth, Social Security Number (SSN)). TAVISS does not maintain criminal history, mental health records, or any other such information regulated by disclosure restrictions. Instead, it merely serves as a method to indicate to one TAVISS user that another TAVISS member agency has a potentially relevant record.

The purpose of the system is to collect information regarding individuals who come to the attention of this agency, as well as other participating agencies in support of their protective mission. Data in the information sharing system is populated by participating law enforcement agencies with information relative to individuals who threaten or exhibit inappropriate behavior towards protected government officials. This information is typically collected by the investigating agency who either obtains it directly from the individual or through investigation of that individual. Any authorized personnel of a TAVISS member agency may input data.

A TAVISS user has the capability to search the system by entering a simple search (name, date of birth and/or identification number) or an advanced search (last name, first name, middle name, DOB, sex, race, National Crime Information Center (NCIC) number, SSN, Alien ID, passport number, state criminal identification number, and/or prison number). The user may also limit their search to those records containing partial data they have available and can modify the search with Boolean logic. A TAVISS record contains the contact information for the agency that entered the subject. The user is responsible for contacting the originating agency and arranging for the exchange of pertinent intelligence information. TAVISS users may also add new records to the system as part of the information sharing program.

The TAVISS system was designed to share a limited amount of information across the participating agencies. The TAVISS system is a web based application with a SQL-Server database. The application server is a Microsoft IIS server. The system was developed as a result of a recommendation made in a U.S. Government Accountability Office (GAO) report in 2000. The system was funded and authorized by Congress in 2001.

Section 1.0 Characterization of the Information

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

The information collected includes the names and identifiers of individuals who come to the attention of member agencies charged with the physical protection of certain government officials.

The TAVISS system may contain any of the following data on a subject:

- Name (first, middle, last)
- Date of birth
- ID number
- Sex
- Race
- NCIC number
- SSN
- Alien ID
- Passport Number
- State ID Number
- Prison Number
- Originating Agency Case Number

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

The information in TAVISS is provided by participating investigative agencies which collect it for their own purposes directly from individuals or indirectly through investigation of individuals.

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

This information is being collected, used, disseminated, or maintained to assist the Secret Service and participating agencies in fulfilling their protective missions by sharing information on individuals who have been involved in incidents or events which relate to protective functions or individuals who have sought to make inappropriate contact with a protectee.

1.4 How is the information being collected?

Any authorized user of a TAVISS member agency may enter data relevant to its investigations directly into TAVISS.

TAVISS users are members of a law enforcement agency engaged in protection pursuant to that agency's specific authorizing federal or state legislation and the rules and regulations applicable to law enforcement agencies.

1.5 How will the information be checked for accuracy?

TAVISS records are not independently checked for accuracy. The accuracy of the information submitted is the responsibility of the reporting agency.

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

The system was recommended in a 2000 report by the U.S. Government Accountability Office (GAO) and funded and authorized by Congress in 2001. The collection of the information is authorized by the Secret Service's protective authority contained in 18 U.S.C. §§ 3056 and 3056A and the Presidential Threat Protection Act of 2000 (Public Law 106-544).

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 TAVISS concern the collection of more PII data than is necessary or erroneous entry of an individual's PII into TAVISS. TAVISS mitigates this risk by limiting access to the system to authorized Secret Service employees engaged in protective intelligence analysis or other authorized individuals of member law enforcement agencies. Of these authorized users, only a subgroup receives additional system rights allowing them to enter records, which is a manual process that requires data entry. The Secret Service enters only those individuals into TAVISS who have been subject to an authorized protective intelligence investigation. Data is most often collected by law enforcement officers directly from the individual in the course of an investigation. The extent of personally identifying information collected by this means depends on the individual's cooperation with investigators. Data may also be obtained lawfully from public or law enforcement records (e.g., existing TAVISS or other agency criminal/protective intelligence record). PII information is collected to enable 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 collected in this system is intended to be shared with participating law enforcement agencies for their investigative use to assist in mitigating potential threats to protected

persons.

Authorized users in the Secret Service query TAVISS for names of individuals that come to the attention of the Secret Service because they have (1) attempted to initiate contact with a protected person in an inappropriate or threatening manner, or (2) the Secret Service received information from a citizen or government agency concerning behavior potentially threatening to protected persons.

The Secret Service enters a TAVISS record for all adult individuals, or juveniles if they have a history of arrests for commission of violent crimes, who are investigated by the Secret Service concerning the risk they may pose to protected persons.

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

No tools are used to analyze the data in, or produced from TAVISS.

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

The system does not directly use any publicly available data. All data provided is entered by member agencies who acquire information in the course of investigations, which may or may not include information from publicly available sources.

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 risk associated with the uses of the information is that users may employ the information for reasons not consistent with the original purpose. To mitigate this risk, member agencies are limited to those with a protective function and within those member agencies an administrator is charged with the responsibility to limit TAVISS access to only those employees with a need-to-know system information for their job function (i.e., managing or conducting investigations of individuals exhibiting potential threatening behavior). Furthermore, at the start of each TAVISS session all participating users are required to affirmatively acknowledge the following responsibilities regarding the use and dissemination of TAVISS records:

- Records are law enforcement sensitive and should not be accessed by or disseminated to non-members;
- Any unauthorized access may be subject to criminal and civil penalties;
- Information exchanged through the system remains the property of and under the legal control of the originating agency; and
- Each participating agency is responsible for its own compliance in collecting, maintaining, and sharing information under the Privacy Act and any applicable regulations.

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?

Names and identifiers of individuals who come to the attention of member agencies charged with the protection of certain government officials.

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 an investigative case file will be retained for a period which corresponds to the specific case type developed (e.g., judicial, non-judicial, non-criminal, etc.).

The retention periods, established and/or approved by the National Archives and Records Administration (NARA), may cover periods as short as two years for individuals investigated by the Secret Service but deemed to pose no risk to protected persons at the time; or as long as 30 years for individuals arrested or committed to a mental institution subsequent to an investigation by the Secret Service. Information which is collected that does not become part of an investigative case file will be destroyed/deleted when it is no longer needed for agency business.

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

Yes, investigative records are retained and disposed of in accordance with various disposition schedules approved by the Secret Service Chief Records Officer and NARA. Consistent with requirements contained within 36 C.F.R. § 1234 and the E-Government Act of 2002, efforts to schedule the electronic system which collects the information have already begun, and the schedule is currently under review by NARA.

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

There is a risk that TAVISS data could be maintained for a period longer than necessary to achieve agency's mission. Although there is always risk inherent in retaining personal data for any length of time, the TAVISS data retention periods based on case type identified in the NARA schedules are consistent with the concept of retaining personal data only for as long as necessary to support the agency's mission. Further, the system is available only to authorized LE agencies, and must be used in conformance with applicable laws and regulations.

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?

TAVISS information may be shared with any eligible DHS component agency becoming a member of the TAVISS network.

4.2 How is the information transmitted or disclosed?

All data is transmitted using secure sockets layer (SSL), 128-bit Encryption. All users must log on using a two-factor authentication.

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.

The main risk associated with internal sharing is unauthorized access to, or disclosure of, PII contained in TAVISS. To mitigate this risk, access to the system is limited to authorized Secret Service employees engaged in protective intelligence analysis or other authorized individuals of DHS agencies with a protective function. DHS policies and procedures are in place to limit the use of and access to all data in TAVISS 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?

The Targeted Violence Information Sharing System (TAVISS) is a shared system directly accessed from remote sites by multiple law enforcement agencies with protective responsibilities for public officials. Each member agency has rights and privileges to alter only those records which they have entered into TAVISS.

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. The system was developed for the purpose of sharing a limited amount of information to law enforcement agencies with protective responsibilities for public officials.

As a protection information system owned by the Secret Service, TAVISS is covered by the DHS/USSS-004 (Protection Information System, 73 FR 77733) System of Records Notice (SORN) which specifies how the information be may used. Also, all Secret Service employees and contractors are trained on the appropriate use of PII. The sharing of information between the Secret Service and participating agencies is covered by and consistent with the routine uses contained in the DHS/USSS-004 SORN.

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

The information is shared between the Secret Service and other participating agencies. The Secret Service bears responsibility for the security of the portal and transmission of the data to participating agencies. Any information shared 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.

In addition, eight primary security standards were established for TAVISS at the outset. These included:

- Identification/Authentication – establishes user accountability and validity of identification
- Auditing – records user activity for after the fact investigation of all transactions
- Accountability – enables security-relevant activities on a system to be traced to individuals who may then be held responsible for their actions
- Availability – assures that data is in the place where the user needs it, when the user needs it, and in the proper form

- Access Control – limits access only to authorized programs and/or systems
- Confidentiality – assures that information is not made available or disclosed to unauthorized individuals, entities, or processes
- Integrity – assures that information has not been altered or destroyed in an unauthorized manner
- Non-Repudiation – Proves delivery or origin of information transactions

Further, security features of the RISS.NET hosting venue comply with the above concerns and include:

- Pointer system directing hits to the entering agency for further information
- Verification that the user is an authorized recognized law enforcement agency
- Commercial VPN software installed on each client's machine
- Token hardware devices (Smart Cards)
- Two Firewalls
- ID and Password
- Mandatory Access Controls
- Discretionary Access Controls
- Weekly Audits
- Virus Scanning
- 128-bit Encryption for Communication

RISS.NET meets all current Secret Service infrastructure security requirements. RISS.NET is a nationwide system maintained by the Department of Justice and designed for sharing multi-jurisdictional criminal intelligence. Its current members include over 6,000 federal, state, and local law enforcement agencies

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

The primary privacy risk associated with external sharing is the sharing of data for purposes that are not compatible with the original purpose of the collection. This risk is mitigated by limiting access to TAVISS to members of authorized law enforcement agencies. When logging on to TAVISS, users must also acknowledge they are accessing a government information system and agree to adhere to rules and regulations concerning information sharing and confidentiality.

Section 6.0 Notice

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

No. Because the information comprising a TAVISS record is collected from the reporting law enforcement agency's records and not directly from the identified individual, the individual is not on notice of the creation of a TAVISS record.

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

No. Individuals have no right to decline to have their information reported to TAVISS by a participating law enforcement agency.

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. This information is part of a law enforcement investigation for protection of public officials.

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.

Notice is not provided to individuals concerning an existence or removal of their TAVISS record in that this information is part of a law enforcement investigation necessary for the protection of public officials and protectees.

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, DHS/USSS-004 SORN permits TAVISS 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 DHS/USS-004 SORN.

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

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

7.3 How are individuals notified of the procedures for correcting their information?

The mechanism for requesting correction of information is specified in the DHS/USSS-004 SORN, published in the Federal Register at 73 FR 77733, in this PIA, and 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 TAVISS is simply an index to participating agencies' records, an individual of record may contest the accuracy and seek the correction of any data with the originating agency through their published mechanisms.

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 TAVISS data is used solely by law enforcement agencies protecting public officials to share available information about individuals who may pose a threat to those officials. Further, the information in TAVISS 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 USSS computers. Access to the information is strictly limited by access controls to those who require it for completion of their official duties.

In addition, eight primary security standards were established for TAVISS at the outset. These included:

- Identification/Authentication – establishes user accountability and validity of identification
- Auditing – records user activity for after the fact investigation of all transactions
- Accountability – enables security-relevant activities on a system to be traced to individuals who may then be held responsible for their actions
- Availability – assures that data is in the place where the user needs it, when the user needs it, and in the proper form
- Access Control – limits access only to authorized programs and/or systems
- Confidentiality – assures that information is not made available or disclosed to unauthorized individuals, entities, or processes
- Integrity – assures that information has not been altered or destroyed in an unauthorized manner
- Non-Repudiation – Proves delivery or origin of information transactions

Further, security features of the RISS.NET hosting venue comply with the above concerns and include:

- Pointer system directing hits to the entering agency for further information
- Verification that the user is an authorized recognized law enforcement agency
- Commercial VPN software installed on each client's machine
- Token hardware devices (Smart Cards)
- Two Firewalls
- ID and Password
- Mandatory Access Controls
- Discretionary Access Controls
- Weekly Audits
- Virus Scanning
- 128-bit Encryption for Communication

RISS.NET meets all current Secret Service infrastructure security requirements. RISS.NET is a nationwide system maintained by the Department of Justice and designed for sharing multi-jurisdictional criminal intelligence. Its current members include over 6,000 federal, state, and local law enforcement agencies

8.2 Will Department contractors have access to the system?

All USSS users of the TAVISS system are USSS employees. All other users must be nominated by the law enforcement agency they work for and be approved by the Secret Service TAVISS administrator.

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 are required to receive annual privacy and security training to ensure their understanding of proper handling and securing of personally identifiable information (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 or 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 Department information systems are audited regularly to ensure appropriate use and access to information. Specifically related to this system, application access is mediated through a two-tier identification and authentication process. End users must successfully gain access to RISS.NET before they can access the TAVISS application. RISS.NET access to TAVISS is restricted to a

population of known user IDs that are generated when the RISS.NET account is issued and manually entered into the TAVISS users table by the system administrator. Both the TAVISS application use and the RISS.NET access account use are audited. Any changes to the hardware or software configuration are subject to review and approval by the Secret Service Configuration Control Board process to ensure integrity of the application.

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?

The risk of unauthorized access exists with any information technology system. Access to TAVISS is restricted to authorized members of member law enforcement agencies with a protective function whose access is controlled through technical identification/authentication via the RISSNET. Information shared via TAVISS is limited to personal identifiers.

Access Control

- Access/control is restricted to users with a valid userid and password. In addition to the userid and password, the user must have an assigned certificate installed on the user's workstation for access through RISS.NET. If the user is on the USSS Network, access is granted via the USSS network active directory account.
- Session timeouts, user selectable from 10 minutes to 4 hours with 30 minutes the system default.
- The account is locked after 3 consecutive incorrect sign on attempts.

Auditing

- All accounts are audited by MAGLOCLEN and TAVISS usage is audited by the TAVISS system administrator.
- The audit trail provides a timestamp and userid.
- The information is recorded into the database for each log on/off attempted.
- The contents of audit logs are protected from unauthorized access, modification, and/or deletion. Administrator privilege is required for access to audit logs.

Section 9.0 Technology

9.1 What type of project is the program or system?

The TAVISS system is an information-collection tool.

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. The system was placed into production in 2004.

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

The project does not employ technology that could raise privacy concerns.

Responsible Official

Richard K. Elias
Assistant Director – Office of Operational Intelligence and Information
United States Secret Service
Department of Homeland Security
Office: 202-406-5725

Approval Signature Page

Original signed copy on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security