Privacy Impact Assessment
for the

U.S. Secret Service Counter Surveillance Unit Reporting Database

DHS/USSS/PIA-004

July 27, 2011

Contact Point
Latita M. Payne
Privacy Officer
United States 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 or USSS) has created the Counter Surveillance Unit Reporting (CSUR) Database. CSUR assists Secret Service employees in managing, analyzing, and distributing intelligence information regarding threats or potential threats to the safety of individuals, events, and facilities protected by the Secret Service. The Secret Service is conducting this Privacy Impact Assessment (PIA) because CSUR contains personally identifiable information (PII) regarding subjects of protective interest to the Secret Service.

Overview

The Protective Intelligence and Assessment Division of the Secret Service manages the CSUR database. The system is used to report and store information collected by USSS Counter Surveillance Units (CSU) and Uniformed Division Officers.

The Secret Service uses CSUs to identify threats against individuals, events, and facilities protected by the Secret Service. The focus of CSU is persons who are showing undue or unusual interest in a protectee or a protected venue. The officer or agent observes, records, and reports information so pre-attack indicators can be revealed, hostile surveillance can be identified, and anomalies can be investigated. Information is gathered from observation of suspicious activity by officers or special agents who are trained to investigate, research, and follow-up on reported information in order to resolve or provide further details about the situation, subject or activity encountered. Occasionally, information in CSUR originates from an information tip from a concerned citizen. That information will only be transferred into CSUR if trained personnel vet the information and determine it is credible and necessary in the furtherance of the agency's protective mission.

The CSUR database is a central repository of information concerning Secret Service agents' and officers' observations of suspicious activity or surveillance directed against Secret Service protectees, events, or facilities. Real-time or on-the-spot feedback may be provided to the field units if deemed necessary. The Secret Service may also use the information in CSUR to investigate, research, and/or follow up on details in order to resolve or provide a clearer picture of the situation, subject, or activity encountered.

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

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

CSUR is covered by DHS/USSS – 004 Protection Information System SORN, 73 F.R. 77733 (Dec. 19, 2008).

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

The certification and accreditation was completed on August 9, 2010, and expires on August 9, 2013.

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

Yes, NARA has approved the records retention schedule for CSUR.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

The information collected in CSUR 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.

The CSUR database is a central repository of information concerning observations of suspicious activity or surveillance directed against individuals, events or facilities protected by the Secret Service. The CSUR database includes the following information, as applicable:

Incident: location, possible direction of interest (protectee, event, or facility), and a narrative description of the suspicious activity.

Individual's (if available): full name, date of birth, age, sex, nationality, race, height, weight, build, eye color, hair length, hair color, facial hair (if any), clothing, street address, e-mail address, telephone number(s), field photographs, and aliases.

Other identifiers that may be recorded in CSUR include information obtained either from the individual or from law enforcement databases such as NCIC/NLETS, including Social Security number (SSN), drivers license number, FBI number, state

criminal ID number, passport number, alien identification number, any other identifying number, and arrest record.

Vehicles: driver, registered owner, color, type, make, model, year, vehicle identification number (VIN), license plate number, the state that issued the license plate, and the year in which the license was issued or renewed.

Some records may contain an address or phone number obtained through conducting a search of commercially available public records, when such information is not otherwise obtained directly through an investigation.

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

Information is gathered from observation of suspicious activity by an officer of the USSS Uniformed Division officer (UND) or a special agent. UND officers at the Joint Operations Center (JOC) relay pertinent information to a UND or CSU member to conduct a follow-up field interview, consent search, or other appropriate action.

Information about suspicious activity may also be provided to the USSS by another law enforcement entity or USSS-vetted observations reported by a concerned citizen.

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

Some records may contain an address or phone number obtained through conducting a public record search, when such information is not otherwise obtained directly through an investigation.

2.4 Discuss how accuracy of the data is ensured.

The accuracy of the information submitted will be checked by the appropriate field unit, working with the CSUR Desk. The field units are comprised of USSS agents and officers trained to investigate, research, and follow-up on reported information in order to resolve or provide further details about the situation, subject or activity encountered.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that the Secret Service could collect information about individuals who pose no threat, particularly via information from non-law enforcement concerned citizens.

Mitigation: Trained personnel vet reported information and only enter into CSUR that

information which is both credible and necessary in the furtherance of the agency's protective mission.

Privacy Risk: CSUR could over-collect PII.

Mitigation: The Secret Service collects the information necessary 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). Information is gathered from observation of suspicious activity or an investigation by an officer of the Secret Service UND or a CSU member. Information about suspicious activity may also be provided to the Secret Service by another law enforcement entity or concerned citizen.

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. CSUR assists Secret Service employees in managing, analyzing, and distributing intelligence information regarding threats or potential threats to the safety of individuals, events, and facilities protected by the Secret Service. The officer or agent observes, records, and reports information so pre-attack indicators can be revealed, hostile surveillance can be identified, and anomalies can be investigated. Officers and agents may conduct searches of data in CSUR and communicate relevant results to Secret Service field units if deemed necessary.

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.

The Secret Service does not use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly.

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

While CSUR database information will be shared with the participants in the (Nationwide Suspicious Activity Reporting Initiative (NSI) Shared Space Environment) facilitated by DHS Information Sharing Environment (ISE) Suspicious Activity Reporting (SAR) via the ISE-SAR Server, there are no other DHS components with assigned roles and responsibilities within the system. Authorized personnel may use the NSI shared space query capability to conduct searches to determine if the subject(s) or

activity has been encountered previously.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a privacy risk of unauthorized access to and inappropriate dissemination of information maintained in CSUR.

Mitigation: The Secret Service has mitigated this risk by implementing primary security standards for CSUR. These include user accountability and validity of identification, user audit logs for significant activity, system time-out after twenty minutes of inactivity, access limited to authorized individuals with a verifiable need to know, account lockout after three bad attempts, and a security warning to users that unauthorized, improper use or access to the system may result in disciplinary action, as well as civil and criminal penalties.

Additionally, trained personnel vet reported information and only enter into CSUR that information which is both credible and necessary in the furtherance of the agency's protective mission. All CSUR users complete annual agency mandated privacy and security training, which stresses the importance of appropriate and authorized use of PII in government systems.

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 System of Records Notice DHS/USSS – 004 Protection Information System SORN, 73 F.R. 77733 (Dec. 19, 2008) provides notice regarding the collection of information and the routine uses associated with the collection of the information. This PIA provides similar notice to the general public as to the collection and use of information for this purpose. Advanced notice of the collection of information to investigative targets or others involved in the investigation generally is not provided as it would compromise ongoing law enforcement investigations and otherwise impede law enforcement proceedings. The final rule for the Protection Information System of Records officially exempts the system from portions of the Privacy Act.

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

Individuals have no right to decline to have their information collected, stored, and maintained in this system. However, they may decline to be interviewed or refuse to provide information requested during the course of an interview.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals are not aware of the existence of CSUR and the data it collects and maintains.

Mitigation: This PIA and the USSS Protection Information System SORN serve as public notice of the existence of CSUR, the data it collects and maintains, and the routine uses associated with the information collected. The information is used only for the purpose for which it was provided through the public notice of this PIA.

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.

Information that is collected that becomes part of an investigative case file will be retained for a period that corresponds to the specific case type developed (e.g., judicial, non-judicial, non-criminal).

The retention periods established and/or approved by the National Archives and Records Administration (NARA) for investigative case files may cover periods as short as two years, or as long as 30 years, depending on the type or disposition of the case.

Per USSS Records Disposition Schedule N1-87-10-4 (approved by NARA on 11/22/2010), CSUR information that has no potential historical or archival value and which does not become part of an investigative file is to be deleted "when the agency determines that it is no longer needed for administrative, legal, audit, or other operational purposes." Understanding that the time frames associated with such purposes can vary widely (e.g., a backup of the database which is overwritten on a nightly basis, versus a litigation-related preservation order which may remain in effect indefinitely), it is not practical to assign a specific retention period to this type of data. However, it should be understood that the Secret Service has no interest in preserving such information any longer than is absolutely necessary.

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 CSUR will be retained for the timeframes outlined in Question 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 general law enforcement system retention schedules 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.

CSUR database information that meet the DHS Information Sharing Environment (ISE) SAR Functional Standard, as outlined in the DHS ISE SAR PIA,[1] will be shared with the participants in the Suspicious Reporting Initiative via the ISE-SAR Server. USSS will enter ISE SAR data by manually. Personnel may use the NSI query capability to conduct searches to determine if the subject(s) or activity has been encountered previously. Also, PII and/or summary investigative information maintained in CSUR may be shared with law enforcement and/or other federal, state, local government agencies who have a need-to-know.

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

Any information maintained in CSUR may be shared in accordance with the purposes and routine uses specified in the Secret Service's System of Records Notice DHS/USSS-04 (Protection Information System, 73 FR 77733) in support of the Secret Service protective mission.

6.3 Does the project place limitations on re-dissemination?

Currently any information maintained in CSUR that is shared with outside law enforcement organizations, and/or other federal, state, local government agencies that have a verified need-to-know is provided via telephone call. Security warnings and disclaimers requiring that the information be kept in law enforcement channels are orally reinforced during the telephone call.

---

[1] U.S. Department of Homeland Security, *Privacy Impact Assessment for the Department of Homeland Security Information Sharing Environment Suspicious Activity Reporting Initiative* (Nov. 17, 2010), http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-dhswide-sar-ise.pdf.

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

When CSUR information is shared with outside law enforcement organizations, and/or other federal, state, local government agencies, an entry is made in the CSUR database record to reflect that the information was shared and with whom it was shared. Information originating from CSUR that is uploaded into ISE SAR may be shared outside of the Department, and records of those disclosures would be maintained by ISE SAR and not CSUR as described in the DHS ISE SAR PIA.[2]

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: The privacy risks associated with this external sharing relates to the unauthorized access to and disclosure of the information maintained in CSUR.

Mitigation: The sharing of information described above is in accordance with appropriate routine uses and legally mandated sharing and will be shared only upon verification of need-to-know and in conjunction with adequate warnings regarding improper re-dissemination.

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, DHS/USSS – 004 Protection Information System SORN, 73 F.R. 77733 (Dec. 19, 2008) permits CSUR to be excluded from the access and redress provisions of the Privacy Act in order to prevent harm to law enforcement investigations or interests. 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 (FOI/PA), 245 Murray Lane, Building T-5, Washington, D. C. 20223, as specified in the Protection Information System 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 Section 7.1.

---

[2] *Ibid.*

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

The mechanism for requesting correction of information is specified in the DHS/USSS – 004 Protection Information System SORN, 73 F.R. 77733 (Dec. 19, 2008), in this PIA, and 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 them under the FOIA and Privacy Act and may also request that their information be corrected. The nature of CSUR 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.

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 are required to receive annual privacy and security training to ensure their understanding of proper handling and securing of PII. 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 Secret Service 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.

8.4 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?

USSS has agreed to contribute CSUR data to the DHS ISE-SAR Server.

Responsible Officials

Richard K. Elias, Assistant Director,
Office of Operational Intelligence and Information
U.S. Secret Service, Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office.

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security