Privacy Impact Assessment
for the

Enterprise Investigative System (EIS)

DHS/USSS/PIA-010

March 30, 2012

Contact Point
U.S. Secret Service
Office of Investigations (INV)
Criminal Investigative Division (CID)
Department of Homeland Security
(202) 406-6350

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) uses the Enterprise Investigative System (EIS) to collect information about ongoing and resolved investigative cases and on individuals seeking access to USSS protected events. EIS is a compilation of six applications that reside on the Secret Service mainframe computer system. The EIS applications are used collectively in support of fulfilling the investigative mission to protect the integrity of the nation's financial systems. These applications are managed by several entities within the Office of Investigations. This PIA is being conducted because the EIS collects personally identifiable information (PII).

Overview

EIS applications serve in fulfilling the investigative mission to protect the integrity of the nation's financial systems. EIS tracks information related to financial/electronic crimes, forged government checks and bonds, as part of criminal investigations. EIS also contains information on background and approval status of applicants, semi-annual review of Secret Service informants, and individuals seeking access to USSS protected events.

The Secret Service utilizes EIS as its central repository for both active and closed investigations. All of the applications that reside within EIS are owned by the Office of Investigation and support the investigative mission. The EIS system includes the collection of data concerning financial-related cases investigated by the Secret Service.

The EIS system includes the following applications that process PII:

- Criminal File Tracking System (CFTS)
  Open investigative files are stored in the Criminal Investigative Division. Daily files are removed from the investigative case vault and presented to region personnel for review and to administrative personnel for updates. Additionally, other Divisions/Offices within Secret Service Headquarters (i.e., Office of Investigations, Legal Counsel, etc.) are provided investigative files for review.

  CFTS is currently located in the Secret Service mainframe. CFTS tracks the physical location of a case file within Headquarters when it is removed by personnel. The application depicts the following information: the case file number, the location of the case file, and the name of current custodian of the case file.

- Event Name Check System

  The Event Name Check System is designed to meet the protective and investigative needs of the USSS. It is used to process single or multiple names to determine suitability into a USSS-protected event. The system provides the USSS with the ability to simultaneously check names through major databases.

The system automates the name check process for users throughout the USSS. Users establish a name list under an event title. The name list will include identifiers for each individual who will be checked (i.e., name, date of birth (DOB), Social Security number (SSN), race, sex, address, telephone). Once all the names have been established under an event, the entire list is submitted for processing.

- Evidence (EVID)
  During the course of a Secret Service investigation, evidence is gathered to support the potential prosecution of unlawful activity. The following items are examples of things gathered for evidentiary purposes: electronics, vehicles, currency, documents, fingerprints, DNA, statements, and video/audio recordings.

  EVID is currently located in the Secret Service mainframe. EVID supports the reporting of all evidenced seized (except Counterfeit Currency). It includes who the evidence is held against, Secret Service certifying names of personnel, a description of the evidence, and disposition of all evidence. EVID is used to print the official SSF1544 - Certified Inventory of Evidence document.

- Forgery System (FORG)
  Secret Service has primary jurisdiction into the forgery, alteration, and theft of U.S. Treasury checks & bonds. Issuing agencies (e.g., Social Security Administration, Internal Revenue Service, etc.) typically receive notification from their customers or by internal notification processes when it is determined that possible criminal activity is occurring. A claim is reported to Financial Management Service-Check Claims Group. An initial screening process of the claim is conducted and, if necessary, a referral is sent to the Secret Service for investigation.

  FORG is currently located in the Secret Service mainframe. FORG is the tracking application used to account for the referrals. The relevant information tracked within FORG is the payee's name and address, the check symbol, the check number, and the date of the check.

- Informants database System (INFRMT)
  USSS uses informants to assist in the investigation of criminal activity. The use of informants is a sensitive matter which requires Special Agents to associate with persons whose motivation and reliability may be suspect. In that regard this investigative technique must be carefully controlled and monitored. The proper use of informants requires that individual rights not be infringed upon and that the Government itself does not become a violator of the law. It is imperative that the Secret Service conduct itself within the parameters of ethical and legal law enforcement behavior.

  INFRMT is currently located in the USSS mainframe. INFRMT contains information on confidential informant/cooperating individual. Policies are mandated by the

Department of Justice and DHS. INFRMT is comprised of the informant's name, date of birth, race, sex, height, weight, address, SSN, phone numbers, and status.

- Master Central Index (MCI)
  MCI processes investigative data. USSS personnel authorized to use MCI can enter data and access information through the Secret Service network.

  MCI contains data which supports both criminal and noncriminal investigations. MCI includes the collection of data concerning numerous aspects of cases handled by the Secret Service including the following: case type, case control limited arrest history, names, date of birth, race, sex, height, weight, eye color, addresses, SSN, phone numbers, and tattoos.

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 following legal authorities:
18 U.S.C. § 1029 *Fraud and related activity in connection with access devices*;
18 U.S.C. § 1030 *Fraud and related activity in connection with computers*;
18 U.S.C. §§ 3056 and 3056A *Powers, Authorities, and Duties of United States Secret Service*;
The Homeland Security Act of 2002, *Public Law* 107-296;
Federal Records Act;
44 U.S.C. § 3101 *Records management by agency heads; general duties*;
5 U.S.C. § 552 *Public information*;
5 U.S.C. § 552a *Record maintained on individuals*;
5 U.S.C. § 301 *Departmental regulations*;
6 C.F.R. Part 5 *Disclosure of Records and Information*; and
42 U.S.C. § 13031 *Child Abuse Reporting*

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

The DHS/USSS-001 Criminal Investigation Information System SORN, 76 FR 49497 provides notice regarding the collection of information and the routine uses associated with the collection of the information. DHS/USSS-004 Protection Information System SORN, 76 FR 66940, applies to the initial name check in the Event Name Check system. If during this process, an individual is flagged as potentially having a criminal record, DHS/USSS-001 would then apply.

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

The system has undergone certification and accreditation, which expires on August 9, 2013.

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

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 Facility Standards for Records and the E-Government Act of 2002, efforts to schedule the electronic system which collects the information have already begun, and the draft schedule will be provided for review by NARA.

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.

This information is not covered by the Paperwork Reduction Act.

Section 2.0 Characterization of the Information

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

- CFTS
  - Case number
  - Case file location
  - Current custodian name
  - Physical location

- Event Name Check System
  - Name
  - DOB
  - SSN
  - Race
  - Sex
  - Addresses
  - Telephone numbers

- EVID
  - List evidence held against
  - USSS certifying names of personnel
  - Description and Disposition of all evidence
  - Print SSF 1544 (Certified Inventory of Evidence Document)

- FORG
  - Payee name
  - Address
  - Symbol and Check number
  - Date of Check

- INFIRM
  - Name of informant
  - DOB
  - Race
  - Sex
  - Height
  - Weight
  - Address
  - SSN
  - Phone numbers

- MCI
  - Case type
  - Case control limited arrest history
  - Names
  - DOB
  - Race
  - Sex
  - Height
  - Weight
  - Eye color
  - Addresses
  - SSN
  - Phone numbers
  - Tattoos

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

The investigative agent or other USSS personnel collects the information directly from individuals or indirectly during the course of an investigation and/or a USSS protected event. The information is extracted from law enforcement databases, commercial sources (e.g., Lexis-Nexis, AutoTrak) and other federal, state and

local law enforcement agencies.

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 collects information during the course of an authorized law enforcement investigation. The 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 employs trained law enforcement agents, officers, and support personnel, who are responsible for ensuring that public or commercial data, along with all case data, is accurate, to the extent possible, before uploading into EIS.

2.4 Discuss how accuracy of the data is ensured.

The information is checked for accuracy during the course of the investigative and/or name check process and again when information is entered into EIS. Personnel must certify the correctness of the information (both when the information is collected and the case is closed) and obtain the appropriate signatures for case disposition. For example, EVID requires three signatures (the person who obtained evidence, the person who witnessed evidence and the supervisor who reviews evidence).

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: A privacy risk associated with this system includes EIS collecting more PII than is necessary.

Mitigation: The risk is minimal because data is most often collected by Secret Service, financial institutions, and/or other law enforcement agencies directly from the individual in the course of an investigative interview and validated through other means (e.g., driver license, birth certificate, Social Security cards, and other witnesses). Data may also be obtained lawfully from other law enforcement records. PII 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). All PII entered and collected is necessary for the purpose of ensuring accuracy in connection with law enforcement investigations and/or the name check process.

Risk: A privacy risk associated with this system concerns the erroneous entry of an individual's PII into EIS.

Mitigation: This risk is mitigated by limiting input and access to the system to authorized Secret Service employees engaged in criminal investigative activities

and the name check process who are trained on the use of EIS.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

- Criminal File Tracking System (CFTS)
  The CFTS tracks the physical location of investigative and personnel files being held within USSS Headquarters (HQ). As files are requested for review or retention their location is tracked for accountability purposes.

- Event Name Check System
  The Event Name Check System is used to process single or multiple names to determine suitability into an event.

- Evidence (EVID)
  EVID uses the information to track evidence collected and processed during an investigation. An individual(s) or entitiy are linked to the evidence.

- Forgery System (FORG)
  FORG uses the information to requests Treasury check information and track the location of where the Treasury check was sent for investigation.

- Informants database System (INFRMT)
  INFRMT uses the information to identify and track the identity of confidential information.

- Master Central Index (MCI)
  MCI uses the information to establish, update, process, search and report details on individuals who are under investigation and/or involved with the investigation.

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.

EIS does not conduct predictive analysis.

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

There are no other components with assigned roles and responsibilities within the

system.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a privacy risk that the information could be compromised and inadvertently accessed by unauthorized individuals.

Mitigation: To mitigate this risk, the information is maintained in a secured system. Access to the information is limited only to those Secret Service employees who need access to effectively perform their jobs.

Privacy Risk: There is a potential risk that EIS information may be used for purposes beyond those stated in 3.1.

Mitigation: To mitigate this risk, policies and procedures are in place to ensure that data is used in accordance with each respective authorized uses for information contained in EIS. All information will be used in conformity with DHS/USSS-001 Criminal Investigative Information System SORN, 76 FR 49497, and in the case of the Event Name Check system, DHS/USSS-004 will apply.

This risk is further mitigated by training all system users on the authorized uses of EIS information. Technical controls and robust auditing capabilities have been implemented to ensure appropriate use and access to information.

Section 4.0 Notice

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-001 Criminal Investigation Information System SORN, 76 FR 49497 provides notice regarding the collection of information and the routine uses associated with the collection of the information.

DHS/USSS-004 Protection Information System SORN, 76 FR 66940, applies to the initial name check in the Event Name Check system. If during this process, an individual is flagged as potentially having a criminal record, DHS/USSS-001 would then apply.

Notice is further provided through the publication of this PIA.

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

Individuals cannot decline having their information collected, stored, and maintained in this system. Individuals do not have the right to consent to particular uses of the information maintained in the EIS.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that subjects of an investigation or those seeking access to USSS-protected events may not know that information about them is being collected and maintained.

Mitigation: The DHS/USSS-001 Criminal Investigation Information System SORN, 76 FR 49497 provides notice of the purpose of collection, redress procedures, and the routine uses associated with the collection of the information. Risks are mitigated through verification and validation during the course of the investigative process and again when information is entered into the EIS. Advanced notice of the collection of their information to investigative targets or others involved in the investigation generally is not provided as it would compromise ongoing law enforcement investigations. In the case of individuals who are seeking access to USSS-protected events, this PIA and DHS/USSS-004 provide notice that background information will be collected and may be disclosed in accordance with the routine uses associated with the collection of the information in order to determine suitability to gain access to a USSS protected event.

Section 5.0 Data Retention by the project

5.1 Explain how long and for what reason the information is retained.

The Secret Service retains the information no longer than is useful or appropriate for carrying out the information dissemination, collaboration, or investigative purposes for which it was originally collected. Information collected which becomes part of a criminal investigative case is retained for a period which corresponds to the specific case type developed (e.g., 30 years for judicial criminal cases; 10 years for non-judicial criminal cases, 5 years for non-criminal cases, etc.). These retention periods, established and/or approved by the NARA may cover periods as short as two years, or as long as 30 years, depending on the type or disposition of the case. Significant and/or unique investigative case-related data of potential historical or archival value is forwarded to the National Archives for permanent retention.

MCI and evidentiary information is currently maintained indefinitely for statistical or historical purposes.

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 EIS will be retained for the timeframes outlined in Question 5.1 to allow the USSS to properly carry out the dissemination, collaboration, or investigative purposes for which the information was originally collected. The retention period is consistent with general law enforcement system retention schedules and is appropriate given the Secret Service's investigative mission.

Section 6.0 Information Sharing

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.

No. The information is not shared outside of DHS as part of the normal agency operations. However, any information maintained in EIS may be shared in accordance with the purposes and routine uses specified in the Secret Service's DHS/USSS-001 Criminal Investigative Information System SORN, 76 FR 49497, and DHS/USSS-004 Protection Information System SORN, 76 FR 66940, for information in the Event Name Check system. For example, investigation information may be routinely shared with DHS Customs and Border Protection and the Department of Justice.

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

The information is not shared outside of DHS as part of the normal agency operations. However, any information maintained in EIS may be shared in accordance with the purposes and routine uses specified in the Secret Service's DHS/USSS-001 Criminal Investigative Information System SORN, 76 FR 49497, and DHS/USSS-004 Protection Information System SORN, 76 FR 66940, for information in the Event Name Check system. To the extent that information may be released pursuant to any 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?

The information is not shared outside of the Secret Service as part of the normal agency operations.

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

Some disclosures of information shared outside of the Secret Service as part of normal agency operations is documented through Memoranda of Understanding (MOUs). For example, information may be shared pursuant to an MOU between the Secret Service and the DOJ, or the Secret Service and NARA.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: To the extent that information may be released pursuant to any routine uses, the privacy risk identified is the disclosure of PII to an unauthorized recipient.

Mitigation: To mitigate this risk, disclosure may only be made by authorized Secret Service employees engaged in law enforcement activities who are trained on the use of EIS. Authorized Secret Service EIS users may only share the data pursuant to routine uses specified in the Secret Service's DHS/USSS-001 Criminal Investigative Information System SORN, 76 FR 49497 in support of the Secret Service investigative mission and DHS/USSS-004 Protection Information System SORN, 76 FR 66940, for information in the Event Name Check system.

Section 7.0 Redress

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

Access is available through written request on a case-by-case basis. Requests should be directed to Communications Center, FOIA/PA Officer, 245 Murray Lane, S.W., Building T-5, Washington, D.C. 20223.

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

The mechanism for requesting correction of information contained in any Secret Service criminal investigation information system is specified in the DHS/USSS-001 Criminal Investigation Information System SORN, 76 FR 49497, and for individuals denied access to a USSS-protected event, in the DHS/USSS-004 Protection Information System SORN, 76 FR 66940, published in the Federal Register, and through a FOIA request

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

The procedures are the same as those outlined in Question 7.2.

7.4 Privacy Impact Analysis: Related to Redress

Redress is available through written request to the Secret Service Freedom of Information Officer if the requestor believes the information maintained by the Secret Service is incorrect. However, pursuant to the needs of law enforcement and the Privacy Act, individual access to and/or correction of existing records may be limited.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

The system is audited regularly to ensure appropriate use and access to information. There are technical safeguards which are installed on workstations such as valid user identification and a corresponding password (with authorized level of security and access privileges).

Additionally, system users must complete annual security awareness and privacy training (and agree to rules of behavior).

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 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. Authorized users are assigned mainframe access levels (with associated system privileges and information access capabilities).

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?

Project review, new sharing agreements, and MOUs are reviewed by subject matter experts, program managers, and appropriate directorate officials.

Responsible Officials

Hugh Dunleavy
Special Agent in Charge
Criminal Investigative Division
U.S. Secret Service
Department of Homeland Security

Approval Signature

Original singed copy on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security