Privacy Impact Assessment
for the

Field Investigative Reporting System

(FIRS)

DHS/USSS/PIA-009

March 7, 2012

Contact Point
U.S. Secret Service
Office of Investigations (INV)
Criminal Investigative Division (CID)
Department of Homeland Security
(202) 406-9330

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 Field Investigative Reporting System (FIRS). The Criminal Investigative Division (CID) is the business owner of FIRS. FIRS consist of seven applications for the reporting of law enforcement activities that fall within the Secret Service's jurisdiction, such as investigating counterfeiting and electronic crimes. The Secret Service is conducting this Privacy Impact Assessment (PIA) because FIRS is a new system that contains personally identifiable information (PII) regarding subjects of criminal investigations.

Overview

FIRS provides field agents the ability to obtain key investigative leads that may originate from many sources. FIRS is designed to support field agents by providing access to information regarding cases, threat assessments, crime patterns, standard operating procedures, and lessons learned at their fingertips. FIRS consist of seven applications to assist the Secret Service with gathering and analyzing key investigative information. The applications are:

- Fastrak application

  During the course of an investigation it may be discovered that assets had been purchased with criminal proceeds. These assets may be subject to forfeiture. Fastrak helps Secret Service personnel manage the entire asset forfeiture process, beginning at the conclusion of the pre-seizure planning stage through to the final disposition of the asset. The application is utilized by the Asset Forfeiture Division.

- In Custody Response (ICR) application

  ICR allows registered users to enter data for cases that have been brought to the attention of the Secret Service by state, local and other federal law enforcement agencies because of a violation within the jurisdiction of the Secret Service. ICR provides a way to capture data for those local arrests or custodial situations where the Secret Service responds but no further investigation is initiated by the Secret Service.

- Electronic Crimes Special Agent Program (ECSAP) application

  A program established within CID to ensure the successful investigation of computer-related and telecommunications crimes in the field, with appropriate oversight from CID.

  The ECSAP application supports the recovery and analysis of evidence from digital storage media. The ECSAP application supports investigations conducted by the Secret Service, by state and local law enforcement agencies, and by other federal law

enforcement agencies. The ECSAP application allows registered users to capture, report on, search for, and review the data for ECSAP cases.

- Wireless Tracking Reporting (WTR) application

  The WTR permits registered users to capture data for wireless phone tracking missions. WTR's include those carried out to support broader Secret Service investigations. Each wireless phone tracking mission is represented by a WTR case.

- Counterfeit Tracking Application (CTA)

  CTA manages data regarding United States counterfeit currency. CTA offers the following features:

  - Unified, flexible searching that provides customized, detailed search results.
  - A complete inventory of all counterfeit contraband of record with the Secret Service, including items both in evidence (IE) and not in evidence (NIE).
  - Integration with the U.S. Dollars website to provide efficient counterfeit processing between financial institutions and the Secret Service.
  - A comprehensive, electronic chain of custody for all inventories of evidence for counterfeit contraband.
  - Access to complete and detailed information - yielded from comparative, forensic exams of counterfeit United States paper currency - in addition to technical data regarding the ink, paper, printing processes, and techniques employed in the simulation of security features.
  - Comprehensive reporting on counterfeit processing statistics, including audit reports and aggregated investigative information.

- Financial Tracking Application (FTA)

  FTA provides real-time fiscal oversight of USSS budgets that are funded by the Treasury Executive Office for Asset Forfeiture (TEOAF). Budgets such as Costs Leading to Seizure (CLS), Purchase of Information/Purchase of Evidence (POI/POE), Major Case Funds (MCF), and Services of Experts & Consultants, are distributed to Secret Service field offices on a case-by-case basis via funding requests submitted through FTA.

- The Comprehensive Incident Database on Targeted Violence (CID-TV)

  The CID-TV is a historical and contemporary catalog of incidents of targeted violence directed toward public officials, public figures, government buildings/facilities, prominent buildings/facilities, hard infrastructure, monuments/landmarks/attractions, and prominent events. The data maintained in the database is limited to information available through open sources (e.g., media,

published case law, and the Internet), and decribes the incident itself, the target(s), as well as the perpetrator(s) and their reported behaviors prior to and during the incident.

- Flipbook application

  The Flipbook is a knowledge-based application that facilitates the security assessment of information systems affecting the safety of persons protected by the Secret Service or the implementation of Secret Service-led security plans. Based on the information collected about an information system, the Flipbook application identifies the risk to the system and makes recommendations for security controls that reduce the risk to the system, thereby reducing the risk to Secret Service protective operations.

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?

Investigative information is solicited and obtained under the authority of the Federal Records Act (44 U.S.C. § 3101) and implementing regulations (Title 36, Code of Federal Regulations, chapter XII). Information is collected from the following types of criminal investigations: financial, counterfeit, and cyber crimes. Such investigations are authorized by 18 U.S.C. §§ 3056 - *Powers, Authorities, and Duties of United States Secret Service*, 1029 - *Fraud and Related Activity in Connection with Access Devices*, and 1030 - *Fraud and Related Activity in Connection with Computers*.

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.

1.3 Has 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?

Various approved record schedules exist which describe and define retention periods for investigative records (e.g., N1-87-89-2, "Field Office Investigative Records Disposition Schedule.") These approved schedules will serve as the basis for a new comprehensive schedule specific to FIRS, which is being developed for approval by the USSS Records Officer and 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.

FIRS collects, uses, disseminates, and maintains the following fields where relevant and available:

- Fastrak application
  - Case Number
  - Cases Agent
  - Court Case Number
  - Disposition Criteria
  - Party Information
  - Seizure Notice
  - Case Name
  - Field Office
  - Adoption Date
  - Party Criteria
  - Claim Information
  - Advertising Announcement
  - Operation Name
  - Seizure Number
  - Forfeiture Criteria
  - Inquiry Criteria

- Petition Information
- Seizure Items

- ICR
  - Case Number
  - City of Offense
  - Date Open
  - Case Synopsis
  - Exams conducted
  - Disposition
  - Statutes Violated
  - Credit Card Info
  - Case Approvers
  - Approval Line
  - Alias
  - Race
  - Eyes
  - Interest to USSS (suspect/subject, payee, witness, etc.)
  - eMail Address
  - ID Number
  - Speech Defects
  - Fingerprints date
  - Misc Numbers
  - Bank Address
  - Address (Primary)
  - Vehicle Information
  - NCIC Check
  - Occupation
  - Military Info
  - DL Number
  - Handwriting
  - Palm prints Date
  - Hobby/Skills (when relevant to a case)
  - Organizations
  - Phone Numbers
  - Employer Info
  - Evidence Info
  - SSN
  - Passport Number
  - Scars/Tattoos/Accent
  - Photograph

- Alien Number
- Bank Acct Numbers
- Affiliations
- Address (Secondary)
- Relatives Information

- ECSAP
  - Case Title
  - State of Offense
  - Evidence Information
  - Disposition
  - Exam dates
  - Approval Info
  - IOD Info
  - Exam Office
  - Case Summary
  - Approvers
  - Case Types
  - Examined Items
  - City of Offense
  - Credit Agent Info
  - Examiners Supervisor
  - Other Agency Info
  - Case Encryption Found
  - Investigative Tools

- WTR application
  - Case Number
  - Case Subject
  - Deployment Status
  - Target Number
  - Provider
  - Pen Register Info
  - Case Types
  - Case Title
  - Tracking Dates
  - Core Violation
  - Phone Located
  - Frequency Band
  - Case Summary
  - Doc Upload

- Originating Office
- Case Jurisdiction
- Parent Case Number
- Other Agency Number
- Tracking Requests Info
- Suspect Apprehended
- After Action Report

- CTA
  - Note Identifiers
  - Rapid Print Number
  - Evidence Info
  - Plant Suppression
  - Release Notes
  - Index Info
  - Batch Info
  - Circular Info
  - Reports
  - Run Out Info
  - Activity Info
  - ICR Case Number
  - Tech Data Info
  - Chain of Custody Info
  - U.S. Dollars Upload

- FTA
  - eMail Templates
  - Funding Allocations
  - Checkbook Info
  - Amounts
  - Status of Requests
  - Descriptions
  - Awardee Info
  - Funding Types
  - Categories
  - Office Info
  - Trans Dates
  - Award Dates
  - Total Costs
  - Status Info
  - TOPS Req Info

- Request Numbers
- Contract Numbers
- Funds Remaining
- Payment Amounts

- CID-TV

  Perpetrators:
  - Name and/or alias
  - Sex/Gender
  - Age at the time of the incident (not DOB)
  - Reported residence at the time of the incident
  - Incident identification number
  - Narrative description of the incident perpetrated as reported by open sources

  Targets:
  - Name
  - Sex/Gender
  - Title
  - Organization

- Flipbook
  - Name
  - Title/role
  - Business email address
  - Business telephone number
  - Business cellular number

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

The information in the system is collected directly from individuals as part of an investigation or indirectly through the investigation of individuals. The various sources are:

- Wireless Tracking Reports: The information is collected from subjects/suspects during the course of tracking mission.
- Electronic Crimes Reports: The information is collected from subjects/suspects during the course of a forensic exam of a computer.
- In Custody Response Reports: The information is collected from subjects/suspects during the course of an investigation, interviews and discussion with other law enforcements.
- Counterfeit Tracking: The information is collected from banks, private entities

and other law enforcement.

- Asset Forfeiture Reports: The information is collected from subjects/suspects and assets being seized during the asset forfeiture processes.
- The Comprehensive Incident Database on Targeted Violence (CID-TV): Informational sources for CID-TV include published media and case law found on Lexis-Nexis or similar online databases, published monographs, professional journals, and the open internet. The information is printed and summarized in CID-TV.
- Flipbook application: The sources of information for the Flipbook application include the personal interview of owners of information systems being assessed as well as open source information.

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

CID-TV uses informational sources that include published media and case law found on Lexis-Nexis and similar online databases. The information is used to document details of past incidents of violence and inform research into preventing future ones.

2.4 Discuss how accuracy of the data is ensured.

The information is checked for accuracy by investigators during the course of the investigative process, and again when information is entered into FIRS.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a privacy risk that more PII may be collected than is necessary to accomplish the purpose for which the information was originally collected.

Mitigation: The risk is mitigated because data is most often collected by Secret Service agents trained in collecting information from various sources which is necessary and appropriate for investigative purposes, whether that information is obtained from individuals, entities, or pre-existing 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).

Privacy Risk: There is a privacy risk of erroneous entry of an individual's PII into the FIRS database.

Mitigation: This risk is mitigated by limiting input and access to the system to

authorized Secret Service employees engaged in criminal investigative activities who are trained on the use of FIRS.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

- Fastrak
  The Fastrak application uses the information to track seized assets through the entire forfeiture process.

- ICR
  The ICR information is used to track criminal activity that falls within the jurisdiction of the Secret Service but does not rise to federal prosecution levels.

- ECSAP
  The ECSAP application uses the information to report the findings of a forensic examination conducted on a subject computer/server (i.e. computer/server identification, HD identification, Media identification, synopsis of examination findings).

- WTR
  The WTR application uses the information to report the results of a wireless tracking mission conducted on a subject phone number (i.e., phone identifier and mission results).

- CTA
  The CTA application uses the information to search and report on counterfeit currency. The information is used to link together notes, and identify trends and passing activity.

- FTA
  The FTA application uses the information to allocate funding to projects, record obligations and expenses, and report funding balances.

- CID-TV
  The CID-TV was created in support of research conducted by the National Threat Assessment Center (NTAC). NTAC was authorized to perform research on targeted violence by the Presidential Protection Act of 2000. The database serves as an historical and contemporary catalog of incidents of targeted violence directed toward public officials, public figures, government buildings/facilities, prominent buildings/facilities, hard infrastructure, monuments/landmarks/attractions, and prominent events. CID-TV will enhance

the agency's level of knowledge in the area of threat assessment by identifying trends, providing information on key incident elements, aiding in the identification of new areas of research, and streamlining the research process for NTAC.

- Flipbook

  The Flipbook application uses the information it collects to assess and mitigate the information security risk to systems that affect the safety of persons protected by the Secret Service or that affect the implementation of Secret Service led protective operations. Specifically, the information collected by the Flipbook application is used to make security control recommendations for information systems as a risk mitigation strategy.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No.

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

No. 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: The privacy risk associated with the uses of the information is the potential that the information could inaccurately identify lawful behavior as suspicious and form the basis of an investigation.

Mitigation: All Secret Service agents are trained to act upon only that information which is both credible and necessary in the furtherance of the agency's protective and investigative missions. Access to the information is limited only to those Secret Service employees who need access to effectively perform their jobs. All Secret Service employees and contractors are trained on the appropriate use of PII.

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. Notice to individuals prior to collection of information could impede law enforcement's investigation. The final rule for the 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 may provide the information voluntarily via consent. Where consent is not obtained, the information is obtained through other lawful means (e.g., search warrant, audio/video recording). Under some circumstances, individuals cannot decline to provide information (e.g., court order). Information obtained during the course of an investigation is maintained in accordance with law enforcement retention rules and policies. Information collected and maintained on individuals can be obtained through the Freedom of Information Act.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that subjects of an investigation 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 general notice of the purpose of collection, redress procedures, and the routine uses associated with the collection of the information.

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 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., 30 years for judicial criminal cases; 10 years for non-judicial

criminal cases, 5 years for non-criminal cases, etc.). Case files involving crimes which have no statute of limitations (e.g., murder) may be retained indefinitely. Information which is derived or received from another law enforcement agency may have specialized retention requirements based upon equities established by the originating agency. (For example, any case file containing Protected Internal Revenue Service Information has a minimum 8 year retention period.)

Information which is collected that does not become part of an investigative case file, per existing retention schedules established and/or approved by the National Archives and Records Administration (NARA), may be destroyed/deleted when no longer needed for administrative, legal, or audit 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: Data may inadvertently be stored for a period longer or shorter than that which is required or necessary.

Mitigation: This risk is mitigated by providing proper records retention training to all system users and periodically auditing the system. The information in FIRS will be retained for the timeframes outlined in Section 5.1 consistent with general law enforcement system retention schedules and necessary to complete the Secret Service's 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.

Yes, any information maintained in FIRS may be shared in accordance with the purposes and routine uses specified in the Secret Service's System of Records Notice DHS/USSS-001 (Criminal Investigative Information System, 76 FR 49497,) in support of the Secret Service investigative mission; for example, investigation information may be routinely shared with the Department of Justice for purposes of prosecution or other law enforcement.

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

Any information maintained in FIRS 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, in support of the Secret Service investigative mission. To the extent that information may be released pursuant to any routine uses, such release may be made only 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?

Yes. When they log on, users of the system are advised that information obtained from the system should be shared only with those individuals or entities that have an official need to know as part of their official responsibilities and that steps should be taken to ensure that the PII contained therein is appropriately safeguarded.

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

Agency policy requires that users of the system document the dissemination of information obtained from the system in their memorandum of record on the matter.

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 be made only by authorized Secret Service employees engaged in criminal investigative activities who are trained on the use of FIRS. Authorized Secret Service FIRS 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.

Section 7.0 Redress

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

Access requests should be directed to Communications Center, FOIA/PA Officer, 245 Murray Lane, S.W., Building T-5, Washington, D.C. 20223 and will be considered on a case-by-case basis. However, as noted in DHS/USSS-001 Criminal Investigative Information System SORN, 76 FR 49497, the system of records is exempt from the Privacy Act's access and amendment provisions; therefore, record access and amendment may not be available in all cases.

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

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

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

The mechanism for requesting correction of information contained in any Secret Service criminal investigation information system is specified in the DHS/USSS-001 Criminal Investigation Information System SORN, 76 FR 49497, published in the Federal Register.

7.4 Privacy Impact Analysis: Related to Redress

Redress may be available by making a 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 in the PA and the DHS/USSS-001 Criminal Investigative Information System SORN, 76 FR 49497.

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 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.

8.2 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 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?

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 signed copy on file with DHS Privacy Office
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security