Privacy Impact Assessment

for the

Field Investigative Reporting System (FIRS)

DHS Reference No. DHS/USSS/PIA-009(b)

February 23, 2023

Homeland Security

Abstract

The United States Secret Service (USSS or Secret Service) is updating the Privacy Impact Assessment (PIA) for the Criminal Investigative Division's (CID) Field Investigative Reporting System (FIRS). FIRS is a suite of tools and applications that facilitates the reporting of law enforcement activities that fall within the Secret Service's jurisdiction. This Privacy Impact Assessment is being updated to document additional data collection sources, including:

1. Commercially available data via USSS Citizen and Law Enforcement Analysis and Reporting License Plate Recognition (CLEAR LPR) service;
2. Social media data;
3. Publicly available data via third-party commercial tools; and
4. National Computer Forensics Institute (NCFI) data to assist local law enforcement (LE) agencies with sponsorship to attend classes offered by the National Computer Forensics Institute.

Overview

FIRS is a consolidated electronic system of investigative information that often serves as the first step in gathering and disseminating investigative data for the Secret Service. FIRS provides registered users with access to capture, store, and search information related to criminal and investigative services, protective services, and, with publication of this Privacy Impact Assessment Update, partner services. Registered users can enter personally identifiable information (PII) into the FIRS system including names, dates of birth, aliases, and Social Security numbers (SSN) related to subjects of criminal investigations, USSS employees, and USSS partners. Personally identifiable information maintained within FIRS falls into one of the following categories: Criminal and Investigative Services, Protective Services, or Partner Services.

The Criminal and Investigative Services category contains case information assigned a unique case number that is linked to personal data, identifying numbers, distinguishing features, investigative data, and work-related data involved in criminal investigations, field intelligence intake, custody responses, informant records, polygraph results, cybercrime information, forensic reports, seized evidence, asset forfeiture, network intrusion responses, and warrant information. Additionally, this category contains information linked to USSS employees, to include training and assignment tracking.

The Protective Services category contains information linked to USSS employees, specifically special agents, including training data, assignment tracking, and trip details, such as

lodging, trip location, and financial reimbursements involved in critical systems protection trips.[1]

The Partner Services category contains information linked to USSS law enforcement partners including personally identifying information, identifying numbers, work-related data, training data, and trip details, such as lodging and trip location. The primary purpose for collecting this information is to validate identity, determine employment status, and confirm eligibility to attend training hosted by the National Computer Forensics Institute, as the National Computer Forensics Institute permits only law enforcement, prosecutors, and judges to attend its training. FIRS is used to register attendees.

Potential risks to privacy may result from improper access to the data or misuse of information in the FIRS system. Accordingly, USSS implemented security features required for system certification and accreditation under the Federal Information Security Modernization Act (FISMA) to meet technical, management, and operational compliance with National Institute of Standards and Technology (NIST) 800-53.

Access, Audit, Identification, and Authentication Controls

Access to the FIRS system is restricted and employs role-based access controls. All system rights, including the rights to read, write, or modify records, are predefined in specific combinations for specific data and associated with specific user roles in the system. Individuals are assigned to a specific system role based on that individual's need to know and the requirements of his or her job description. Individual assignment to specific roles requires the approval of the FIRS application owner or FIRS System Owner. Once approved, the FIRS application owner or FIRS Administrator assigns applicable roles to the user. FIRS uses multifactor authentication and performs user authentication each time a user logs in. Once authenticated, the user is granted access to the applications within FIRS based on his or her assigned role(s). Each user is uniquely defined, and auditing activities include login successes and failures.

FIRS users are required to review and understand the FIRS Rules of Behavior and other directions for proper use of the system, and are also required to complete annual training to ensure they properly handle and protect personally identifiable information. User manuals and training on protecting personal information, security awareness, and rules of behavior are provided to users on an annual basis, in adherence with DHS privacy practices and policies. DHS has also published the Handbook for Safeguarding Sensitive Personally Identifiable Information, providing personnel with additional guidance.[2]

---

[1] Critical systems protection trips are used to assess and mitigate risk of cyberattacks to computer networks, critical infrastructure, and information systems that could have an adverse effect on or disrupt the USSS physical security plan.

[2] *See* U.S. DEPARTMENT OF HOMELAND SECURITY HANDBOOK FOR SAFEGUARDING SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION (2017), *available at* https://www.dhs.gov/publication/handbook-safeguarding-sensitive-personally-identifiable-information.

Memoranda of Understanding (MOU) or Interagency Service Agreements (ISA) are in place with each agency or entity with whom the USSS routinely shares FIRS information. These documents are reviewed periodically by subject matter experts, program managers, and appropriate directorate officials and updated, as needed. They stipulate how the information must be handled by the external sharing partners based on the controls for the original collection of information by referencing security policies, roles and responsibilities, retention, and contact lists.

Access to non-DHS approved removable media (e.g., CDs, USB drives) is prohibited. Any DHS approved media used must be sanitized prior to reuse or disposal. The database that retains FIRS information is maintained under the Application Provision System (APS)[3] and is encrypted-at-rest. If suspicious activity is noted from auditing, the logs are reviewed by system and security personnel and necessary actions are taken.

Reason for the PIA Update

The Privacy Impact Assessment is being updated to document the following system changes since the last Privacy Impact Assessment Update in November 2016:[4]

1. **Usage of commercially available data via USSS CLEAR License Plate Recognition (CLEAR LPR) service.** The USSS Criminal Investigative Division (CID) leverages the DHS Research Library and Information Services (RLIS) to access license plate information obtained from commercially available fixed and mobile license plate reader technology to assist in locating subjects under investigation. "Subject under investigation" means a person, place, or thing that can be uniquely identified by name and has some relationship to criminal activity that is the subject of a criminal investigation. If data is determined to be applicable to a Secret Service criminal investigation, the relevant data is manually added to the appropriate FIRS application.

2. **Usage of social media data.**[5] USSS uses social media to gather information related to subjects of criminal investigations by researching publicly available,[6] open-source social media data. If determined to be relevant to a Secret Service criminal investigation, the relevant data is manually added to the appropriate FIRS application.

---

[3] The Application Provisioning System is a three-tiered software design/architecture focused on ingesting, processing, and analyzing raw data that is collected from various USSS investigative and protective data sources.
[4] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, UNITED STATES SECRET SERVICE, PRIVACY IMPACT ASSESSMENT FOR THE FIELD INVESTIGATIVE REPORTING SYSTEM, DHS/USSS/PIA-009 (2012 and subsequent updates) *available at* https://www.dhs.gov/privacy-documents-us-secret-service.
[5] USSS adheres to DHS Privacy Policy for Operational Use of Social Media, *available at* https://www.dhs.gov/publication/privacy-policy-operational-use-social-media-directive-110-01.
[6] DHS defines "publicly available information" as unclassified information that has been published or broadcasted in some manner to the general public, is available to the public by subscription or purchase, could lawfully be seen or heard by a casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event that is open to the public. *See* DHS Lexicon, Revision 2 (2017), *available at* https://www.dhs.gov/publication/dhs-lexicon.

3. **Usage of publicly available data via third-party commercial tools.** These commercial tools consist of databases, software programs, or web-based tools that are used to develop investigative leads. These tools search for information about people and their affiliations, businesses, criminal records, court records, and assets which provide the capability to search and aggregate other relevant public and commercial data based on unique identifiers. If determined to be applicable to Secret Service criminal investigations, the information generated and aggregated using these tools is noted in the appropriate FIRS application.

4. **Usage of National Computer Forensics Institute data.** This data is collected to assist local law enforcement agencies with sponsorship to attend classes offered by the National Computer Forensics Institute. Local law enforcement agencies throughout the United States provide their information for nomination and registration for National Computer Forensics Institute classes. Relevant data is manually added to the appropriate FIRS application.

Privacy Impact Analysis

Authorities and Other Requirements

The authorities for collection of information housed within FIRS remains unchanged with this update. The DHS/USSS-001 Criminal Investigation Information System of Records Notice (SORN)[7] applies to the FIRS criminal information. The DHS/USSS-004 Protection Information System of Records Notice[8] applies to information regarding critical systems evaluations for protective trips. These System of Records Notices notify the public that data is obtained from commercial and public sources, among other sources, and prescribes permissible routine uses for the information.

Characterization of the Information

FIRS collects and retains the following information in the Criminal and Investigative Services category, as relevant and applicable to an investigation:

- Full Name
- Address(es)
- Phone Number(s)
- Email Address(es)
- Social Security number (SSN)

[7] *See* DHS/USSS-001 Criminal Investigation Information, 85 Fed. Reg. 64523 (October 13, 2020), *available at* https://www.dhs.gov/system-records-notices-sorns.
[8] *See* DHS/USSS-003 Protection Information SORN, 85 Fed. Reg. 64519 (October 13, 2020), *available at* https://www.dhs.gov/system-records-notices-sorns.

- Alias
- Social Media Names/Information
- Military Service
- IP Addresses
- A-Number Registration
- Driver's License
- Passport Number
- Financial Account Information
- FBI Number
- Place of Birth
- Race/Ethnicity
- Tax Identification Number (TIN)
- Date of Birth (DOB)
- Physical Descriptions/Identifiers (e.g., Height, Weight, Sex, photos, fingerprints)
- Physical Characteristics/Identifying Marks & Disfigurements
- Work-Related Data (e.g., Occupation, Work Address)
- Vehicle Descriptions (e.g., Make, Model, License Plate, VIN, location)

This information in the FIRS system is collected directly from individuals as part of an investigation or indirectly through the investigation of individuals. This Privacy Impact Assessment is being updated to account for other methods of collection including usage of commercially available data, social media data, publicly available data, and National Computer Forensics Institute data. All data is collected and entered manually or uploaded into the appropriate FIRS application. The FIRS system does not ingest data through bulk collection.

Data that is available through commercially available sources, publicly available sources, and social media is analyzed and reviewed by USSS investigative personnel. If data is determined to be applicable to a criminal investigation, the relevant data is manually entered into the appropriate FIRS application.

This data may include License Plate Reader data. License Plate Reader data is accessed via a DHS subscription contract that components may leverage pursuant to their authorities and obtained through a third-party vendor via the CLEAR database. The CLEAR database provides access to vehicle license plate data captured from cameras throughout the nation. This information

is converted into alpha numeric data and stored in a database with the associated location (e.g., Global Position System (GPS) coordinates) of the image capture as well as the associated date and time of the capture. All data is stored in an electronic database accessed by verified users with unique user credentials. Only License Plate Reader data identified as relevant to a USSS investigation will be indexed and stored in the appropriate FIRS application. Within FIRS, USSS personnel document details about how the data was accessed (e.g., date searched, search parameters, results). In the CLEAR database, the USSS can run a geographic query, enter a partial license plate query, and utilize a mobile application to conduct queries (i.e.by scanning a license plate and searching the CLEAR database for that license plate). The USSS does not capture or input any license plate data into CLEAR's source commercial databases.

FIRS collects and retains the following information in the Protective Services category:

- Full Name
- Address(es)
- Phone Number(s)
- Email Address(es)

This information in the FIRS system is collected directly from investigators as part of a critical systems protection trip assessment. Investigators check the information for accuracy during the assessment and again when the information is entered into FIRS. Additional checks are conducted by the Criminal Investigative Division. Automated checks are embedded into the tools to ensure accuracy of the data.

FIRS collects and retains the following information in the Partner Services category:

- Full Name
- Address(es)
- Phone Number(s)
- Email Address(es)
- Social Security Number
- Partner Organization

This information is collected directly from the law enforcement partners as part of the registration process for applying to attend a USSS National Computer Forensics Institute class, for task force membership, or other USSS partnerships.

Partners check the information for accuracy during the registration process. Additional checks are conducted by Field Office supervisors, Field Office administrative personnel, and the

Criminal Investigative Division. Automated checks are embedded into the tools to ensure accuracy of the data. Additionally, each office certifies their partner information quarterly.

Privacy Risk: There is a risk that information collected from social media and commercially available sources might contain inaccurate information, leading USSS to store it in FIRS and rely on inaccurate data in furtherance of its law enforcement mission.

Mitigation: The risk is partially mitigated. USSS does not take enforcement action against any individual based solely on the information obtained from social media and/or commercially available sources. Authorized USSS personnel receive training to verify all accessed data is relevant to ongoing investigative and enforcement activities. Investigators check the information for accuracy during the investigation process, and again when the information is entered into FIRS. Authorized USSS personnel also check the information against such sources as pre-existing law enforcement records before taking any action against the individual. Additional checks are conducted by Field Office supervisors, Field Office administrative personnel, and the Criminal Investigative Division. Automated checks are embedded into the tools used by FIRS to ensure accuracy of the data. If the data is determined to be inaccurate, it is deleted from FIRS and not relied on in the investigation. If the inaccurate data was further disseminated by USSS personnel involved with the case, they would notify the receiving parties.

Privacy Risk: There is a risk that License Plate Reader technology query results might contain inaccurate information, leading USSS to store it in FIRS and rely on inaccurate data in furtherance of its law enforcement mission.

Mitigation: The risk is partially mitigated. USSS does not take enforcement action against any individual based solely on the information obtained from the License Plate Reader service. Authorized USSS personnel receive training to verify all accessed data is relevant to ongoing investigative and enforcement activities. Investigators check the information for accuracy during the investigation process and again when the information is entered into FIRS. Additional checks are conducted by Field Office supervisors, Field Office administrative personnel, and the Criminal Investigative Division. Automated checks are embedded into the tools to ensure accuracy of the data. If the data is determined to be inaccurate, it is deleted from FIRS and not relied on in the investigation. If the inaccurate data was disseminated by USSS personnel involved with the case, they would notify the receiving parties.

Privacy Risk: There is a risk that more information than necessary will be entered into FIRS.

Mitigation: The risk is mitigated. Although the new features described in this Privacy Impact Assessment afford USSS personnel with access to more information, only that data deemed relevant and necessary to a criminal investigation, protective, or partnership activity is entered into FIRS. Secret Service personnel are trained to assess data from multiple sources (i.e., from

individuals, entities, or pre-existing law enforcement records) and determine which data is necessary and appropriate for their investigation, and then only retain and use the information that meets that standard. Personally identifiable 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.

Privacy Risk: There is a risk that information will be inaccurately manually entered into FIRS.

Mitigation: This risk is partially mitigated. All information is reviewed prior to finalizing its input into FIRS, in accordance with USSS standard operating procedures. Additionally, access to FIRS is only granted to authorized Secret Service employees engaged in criminal investigative or protective activities who are trained on the use of FIRS.

Uses of the Information

FIRS is a consolidated electronic system of investigative information that often serves as the first step in gathering and disseminating investigative data for the USSS. FIRS provides registered users with access to capture, store, and search information related to criminal and investigative services, protective services, and partner services. The Secret Service relies on a variety of law enforcement tools and techniques in support of its integrated criminal and protective missions.

Social media is used as relevant to and primarily to enhance the investigation on an individual, to provide situational awareness in an ongoing criminal investigation, and to assist in determining how to proceed in the investigation. Commercial License Plate Reader data is used when the status of an investigation so warrants, for example, when the current or past location of the subject or a vehicle is relevant to the case. The purpose of leveraging the DHS License Plate Reader subscription contract via the CLEAR database is not to use it in every case; in some cases, no license plate information will be available to investigators to query and in other cases it may not be needed.

Privacy Risk: There is a risk that the information accessed through social media or commercial tools/subscriptions and saved in FIRS may be used improperly.

Mitigation: This risk is mitigated. All Secret Service agents are trained to act upon only that information which is both credible and necessary in furtherance of a criminal investigation or protective activity. Access to the information is limited only to those Secret Service employees who need access to effectively perform their jobs in furtherance of a criminal investigation or protective activity. Additionally, all Secret Service personnel are annually trained on the appropriate use of personally identifiable information. Further training is provided for those personnel using the CLEAR database and License Plate Reader functionality.

Notice

This Privacy Impact Assessment provides notice of these USSS activities. The above-mentioned USSS System of Records Notices provide notice regarding the collection of information and the routine uses associated with the collection of the information. However, specific notice to individuals prior to collection of information could impede ongoing law enforcement investigations, so such direct notice is not provided.

Individuals may provide the information voluntarily via consent during investigative interviews. Where consent is not obtained, the information is obtained through other lawful means (e.g., legal process), use of third-party commercial services (CLEAR, LexisNexis), or via open source (publicly available) information located on social media platforms. Under some circumstances, individuals cannot decline to provide information (e.g., legal process). Information obtained during an investigation is maintained in accordance with law enforcement retention rules and policies. Information collected and maintained on individuals can be requested through the Freedom of Information Act.

Privacy Risk: There is a risk that individuals will not know that USSS is collecting information through social media or from commercially available sources.

Mitigation: This risk is partially mitigated. This Privacy Impact Assessment and associated System of Records Notices provide a measure of notice to the public. USSS does not provide direct notice or obtain direct consent from individuals when collecting data from social media or commercially available sources in support of a criminal investigation or protective activity.

Data Retention by the Project

FIRS adheres to the appropriate USSS Investigative and Protective Retention Schedule. These schedules cover investigative records relating to USSS criminal investigations, as well as non-criminal and internal USSS investigations, and protection operations. Relevant retention schedule numbers are: N1-087-89-002, N1-087-92-002, and N1-087-11-2.[9]

The Secret Service does not retain information any longer than is useful or appropriate for carrying out the purposes for which it was originally collected. Information that is collected and becomes part of an investigative case file will be retained for a period that corresponds to the specific case type. Case files involving crimes that have no statute of limitations may be retained indefinitely. Information that is derived or received from another law enforcement agency may have specialized retention requirements based upon equities established by the originating agency.

[9] *See* https://www.archives.gov/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0087/n1-087-89-002_sf115.pdf and https://www.archives.gov/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0087/n1-087-92-002_sf115.pdf.

Information collected that does not become part of an investigative case file, per existing retention schedules established and approved by the National Archives and Record Administration (NARA), will be destroyed/deleted when no longer needed for administrative, legal, or audit purposes.

Information Sharing

Memoranda of Understanding or Interagency Service Agreements are in place with each agency with which the USSS routinely shares FIRS information. These documents are reviewed by subject matter experts, program managers, and appropriate directorate officials periodically and updated as needed. They indicate how the information must be handled by the external sharing partners based on the controls for the original collection of information by referencing security policies, roles and responsibilities, retention, and contact lists.

Information maintained in FIRS may also be shared outside of DHS with other federal, state, local, and foreign agencies for law enforcement purposes on a case-by-case basis. Any information shared from FIRS to external law enforcement entities occurs under existing agreements. Such sharing will take place only after USSS determines that the receiving component or agency has a need to know the information to carry out national security, law enforcement, immigration, intelligence, or other functions in accordance with the purposes and routine uses specified in the Secret Service System of Record Notices listed above, in support of the Secret Service mission. For example, investigation information may be routinely shared with the Department of Justice for purposes of prosecution or other law enforcement purposes. 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 purpose of the original collection, as determined on a case-by-case basis.

Information maintained in FIRS is shared with recipients who have a need-to-know in the performance of their official duties. Security warnings requiring that the information be kept in law enforcement channels are orally reinforced during telephone calls. Additionally, the USSS routinely marks its investigative documents as "law enforcement sensitive (LES)—not for further dissemination without permission."

By policy and user training, users are instructed to record each instance a disclosure is made outside of DHS. FIRS also includes a disclosure reminder. USSS policy requires that FIRS users document dissemination in a memorandum of record. The FIRS user specifies details about the information obtained, when it was obtained, and how it was obtained in the dissemination report. For example, the FIRS user would include in the report details such as: 'On 11/29/2022, I conducted a search of XXXX on Social Media Site YYYY, which rendered the reported results.'

Redress

Access and amendment 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, both USSS system of records are exempt from certain aspects of the Privacy Act's access and amendment provisions; therefore, record access and amendment may not be available in all cases.

The mechanism for requesting correction of information contained in any Secret Service criminal investigation information system is specified in the System of Records Notices published in the Federal Register and available at: https://www.dhs.gov/system-records-notices-sorns.

Auditing and Accountability

Documentation and required annual training ensure personally identifiable information in FIRS is appropriately handled and secured. User manuals and annual trainings such as protecting personal information, security awareness, and IT rules of behavior, are provided to users so that they adhere to appropriate privacy practices and policies. DHS has also published the Handbook for Safeguarding Sensitive Personally Identifiable Information, providing personnel with additional guidance.

DHS physical and information security policies dictate who may access Secret Service computers and filing systems. Specifically, DHS Management Directive 4300A[10] 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.

USSS has responsibility for auditing personnel utilizing third-party commercial services to obtain data that includes data for entry into FIRS. USSS system administrators request an audit of user activity through the vendor or if a user trips an alert. An audit then will be automatically conducted by the vendor and reported back to USSS. Commercial data services employed by the USSS have in place at a minimum Levels of Agreements (LOAs) that include auditing and other security controls. Auditing data includes the identity of the user initiating the query or the person on whose behalf the query is initiated, if different, and usage logs. Account data can be accessed for up to five years following the deactivation of an account. Audits conducted on users also can detect queries inconsistent with authorized uses. Further, USSS personnel suspected of violating

[10] DHS 4300A Sensitive System Handbook is a series of information security policies, which are the official documents that create and publish Departmental security standards in accordance with DHS Management Directive 140-01, Information Technology System Security. *See* U.S. DEPARTMENT OF HOMELAND SECURITY, DHS 4300A SENSITIVE SYSTEMS HANDBOOK, *available at* https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook.

the authorized use of these services will be referred to the USSS Inspection Division for investigation and possible disciplinary action.

Contact Official

Christal Bramson
Privacy Officer
U.S. Secret Service
privacy@usss.dhs.gov

Responsible Official

Jason Kane
Special Agent in Charge (SAIC)
Criminal Investigative Division (CID)
United States Secret Service

Approval Signature

Original, signed copy on file at the DHS Privacy Office.

_____

Mason C. Clutter
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717