Privacy Impact Assessment Update
for the

eAgent

DHS/USSS/PIA-015(a)

April 26, 2017

<u>Contact Point</u>

Latita Payne
Disclosure and Privacy Officer
U.S. Secret Service
(202) 406-5838

<u>Reviewing Official</u>

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The United States Secret Service (USSS) is updating the Privacy Impact Assessment (PIA) for the Enterprise Agent (eAgent) system in order to document additional sources of information and the collection of personally identifiable information (PII) of individuals who will be in proximity to a USSS protectee. The eAgent system is a USSS-owned Commercial Off-the-Shelf (COTS) web-based application used by personnel within the Investigative and Protective Divisions to access the National Criminal Information Center (NCIC) and the National Law Enforcement Telecommunications System (Nlets). eAgent consists of two major components, the Message Switch System (MSS) and Apache web server. The primary function of eAgent is to facilitate direct access to critical information, such as criminal records and the status of wanted individuals, to requesting authorized USSS personnel in a timely manner.

Overview

USSS is mandated by statute[1] to protect dignitaries and investigate crimes against the United States financial system. In order to meet these mandates, the eAgent application facilitates timely access for USSS personnel to the NCIC[2] and Nlets[3] data services. The eAgent system assists Secret Service personnel in performing record checks of USSS data against NCIC and Nlets. Additionally, eAgent allows USSS personnel to input information about individuals obtained during the course of law enforcement encounters, background investigations, or protective activities, which can then be shared with NCIC and Nlets stakeholders. eAgent allows USSS personnel to run multiple queries simultaneously. For instance, when USSS personnel query a license plate number, eAgent can run additional queries such as vehicle registration, stolen vehicle reports, and wanted person information simultaneously.

The USSS Information Resources Management Division is the business owner of eAgent. Within USSS, eAgent is used primarily by personnel in the Investigative and Protective Divisions. USSS personnel collect PII pertaining to individuals who are encountered, arrested, in custody, or

[1] *See* 18 U.S.C. § 3056, as amended, "Powers, authorities, and duties of the United States Secret Service;" 18 U.S.C. § 3056A "Powers, authorities, and duties of the United States Secret Service Uniformed Division;" 18 U.S.C. § 1029(d) "Fraud and related activity in connection with access devices;" and 18 U.S.C. § 1030(d) Fraud and related activity in connection with computers).

[2] NCIC is a nationwide information system established by the Federal Bureau of Investigation (FBI) to assist criminal justice agencies. The system is a computerized index of information on crime and criminals of nationwide interest, and a locator file for missing persons that assists USSS by providing and maintaining a computerized filing system of accurate and timely documented criminal justice information. *See* http://www.fbi.gov/about-us/cjis/ncic for more information about NCIC.

[3] Nlets, a computer-based message switching system, links local, state, and federal law enforcement agencies, selected international agencies, and a variety of strategic partners for the purposes of sharing and exchanging critical information. Nlets does not maintain records, but rather it provides USSS and other user agencies with the means to confirm data and transmit law enforcement, criminal justice, and public safety-related information securely in a standardized format for law enforcement information sharing purposes. See https://www.nlets.org/ for more information about Nlets.

under investigation; individuals who are the subject of a special security event check or who will be in proximity to a USSS protectee; and individuals for whom USSS is performing a background investigation. USSS personnel primarily use eAgent as a gateway to NCIC to create, update, and clear records in NCIC about persons for whom USSS has an outstanding criminal warrant or protective intelligence lookout. A USSS-generated record is "cleared" in the NCIC system when the subject is located or arrested, which indicates that the search for the subject is no longer active. A "cleared" status does not mean that the record is deleted from NCIC; rather instead that the subject has been located.

USSS users of eAgent from the Investigative Support Division (ISD) are able to modify records in the NCIC and may enter PII such as name, date of birth, vehicle identification number, or license plate number to update the NCIC system, which ensures USSS-generated NCIC records are current and complete for inquiries by law enforcement agencies. Other USSS personnel use eAgent to query NCIC in order to access and exchange information transmitted through the Nlets network to identify individuals, determine if they are wanted by other law enforcement agencies for suspected criminal activity, and generate investigatory leads for further action. USSS personnel may also run criminal history inquiries, driver's status, and wanted status checks on persons of interest to USSS.

Users of the eAgent system may also view images within NCIC to help USSS identify people and property items. USSS users may view images without any automated facial recognition capabilities. The Interstate Identification Index, which contains automated criminal history record information, is accessible through the same network as NCIC and is stored in the eAgent Manageable Archive of Retrievable Transactions (MART) database[4] with the original query.

Finally, USSS personnel use eAgent to send out messages across Nlets. The alert messages request additional information, seek assistance from other law enforcement agencies, or respond to a request from another agency. For example, law enforcement agencies confirm wanted status and warrants via the Nlets Hit Confirmation function. Such alerts may contain PII, such as name, driver's license number, date of birth, or any information that may identify a subject as listed under characterization of the information.

Standard queries made by USSS personnel to NCIC via eAgent return information contained in NCIC files and in databases that are connected to Nlets. If a record exists, USSS agents and officers confirm the status of the information with the originating agency and use the PII to determine appropriate actions to take, such as arresting the individual or seizing property.

[4] The eAgent MART database archives copies of the data retrieved from NCIC at the moment in time when the query was made. These records are maintained in the eAgent database for auditing purposes, to exactly identify the information available at the time of the query.

In some cases the information returned from the query is limited and the USSS users contact the originating agencies for additional details on positive matches.

The eAgent system consists of two components: a Message Switch System (MSS) that interfaces with both NCIC and Nlets, as well as an application that routes queries to NCIC and Nlets through a browser-based user interface, which is available via desktop or laptop computers on the USSS network. Each transaction sent to and from NCIC and Nlets is logged in the MART database, which functions as eAgent's transaction archive. Authorized advanced users may perform inquiries on transactions run in the MART and view a log of the PII routed to and from NCIC and Nlets for audit and quality control purposes. The MART audit records for eAgent store all information used to query, in addition to any modifications made to NCIC records.

Reason for the PIA Update

DHS is updating the eAgent PIA to document the use of open source[5] information on individuals who will be in proximity to a USSS protectee. The collection of this additional information will help USSS personnel verify the identities of individuals in proximity to protectees, as well as assist in the identification and investigation of any potential threats they may pose. USSS collects information directly from individuals, third parties, and open sources, including social media, during the course of a law enforcement encounter, a background investigation, special security event check, or when an individual will be in proximity to a USSS protectee. Other than the transaction log in the MART database, USSS only retains information from eAgent record checks that is required for further investigation. In the event of an investigation, USSS personnel, who have specialized training in investigative and analytical techniques, review all pertinent information and conduct research to verify the information, including the accuracy of the collected PII, in order to further the USSS mission.

Privacy Impact Analysis

In each of the below sections consider how the system has changed and what impact it has on the below fair information principles. In some cases there may be no changes and indicate as such.

Authorities and Other Requirements

There are no changes in the specific legal authorities and agreements that permit and define the collection of information in eAgent. Information is collected per the Secret Service's investigative and protective authority contained in 18 U.S.C. §§ 3056 and 3056A, Powers, authorities, and duties of United States Secret Service; Powers, authorities, and duties of United States Secret Service Uniformed Division. Memoranda of Agreements (MOA) with the NCIC and

[5] Open source information is "unclassified information that has been published or broadcast in some manner to the general public, 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."

Nlets govern network interface and protocol requirements and shared access/query and update capabilities.

Characterization of the Information

As described in the July 17, 2015 PIA, the eAgent system maintains fourteen types of "person files" containing records of individuals in NCIC including: Supervised Release; National Sex Offender Registry; Foreign Fugitive; Immigration Violator; Missing Person; Protection Order; Unidentified Person; U.S. Secret Service Protective; Gang; Known or Appropriately Suspected Terrorist; Wanted Person; Identity Theft; Violent Person; and National Instant Criminal Background Check System (NICS) Denied Transaction.

The eAgent interface allows ISD users to modify records within NCIC. Other USSS users of eAgent are able to retrieve the following information from NCIC, but they cannot modify records. USSS may query (and modify, if an ISD user) the following records from NCIC:

- Full name;
- Sex;
- Race;
- Height;
- Weight;
- Scars, marks, tattoos, and other characteristics;
- Eye color;
- Warrant number;
- Criminal history;
- Image (for example, mugshot, right index fingerprint, and signature);
- Vehicle Registration Number;
- License Plate Number;
- Driver's License Number;
- Date of birth;
- Place of birth;
- Address;
- Occupation;
- Social Security number;
- State Identification Number;
- FBI Number (number assigned by the FBI to an arrest fingerprint record);
- Miscellaneous identification numbers such as Passport Number, Military ID, etc.; and
- Information contained in the Interstate Identification Index.

eAgent users may query fields for or receive back the following information from Nlets:

- Full name;
- Date of birth;
- State criminal history;
- Vehicle/boat registration;
- State identification number;
- Driver's license number; and
- INTERPOL information such as international warrants, stolen vehicles, stolen passports, and other travel documents.

USSS collects information directly from individuals during the course of a law enforcement encounter, through background investigations and special security event checks, or from open sources (court records, real-estate records, etc.) and third parties (i.e., other agencies, private sector, employers, etc.) in an effort to identify individuals who will be in proximity to a USSS protectee, as well as complete records checks and verify the identity of those individuals. USSS personnel then enter the information into eAgent to perform the records check. Some information may be collected by other law enforcement agencies and passed to USSS in NCIC. Information in eAgent is also obtained from law enforcement agencies that seek additional information about a USSS-generated NCIC record or for an NCIC hit confirmation. Additionally, law enforcement agencies may contact USSS if they wish to report suspected violations. Information maintained within eAgent MART is obtained from responses to the queries made to the NCIC and Nlets systems.

All records entered by ISD in NCIC are validated annually to comply with NCIC requirements. NCIC sends a list of entries that need to be validated to the NCIC Program Manager who then distributes them to assigned Terminal Access Coordinators (TAC) in each field office. The TACs are responsible for validating these records in a timely manner in accordance with a deadline set by NCIC. The validation process is accomplished by reviewing the entry and current supporting documents, as well as through consultation with the complainant, victim, prosecutor, court, or other appropriate source. USSS confirms with NCIC that the records are complete, accurate, and still outstanding, or active upon completion of this process. Additionally, when another law enforcement agency contacts USSS regarding a USSS-generated NCIC record, a USSS employee confirms if the warrant is still valid and assists the locating agency in determining if the subject in custody or under investigation is the same person identified in the USSS-generated record.

Privacy Risk: There is a privacy risk that more PII may be collected than is necessary to accomplish the investigative and protective purposes for which it was originally collected.

Mitigation: Secret Service agents and officers are trained to collect only the necessary and appropriate PII for investigative and protective purposes. 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. Information is gathered on individuals based on observations of suspicious activity, an investigation by an officer of the Secret Service, a referral from another agency, or from open sources or a third party regarding individuals who will be in proximity to a USSS protectee. Information about suspicious activity may also be provided to the USSS by another law enforcement entity or concerned citizen, which may prompt additional information gathering using eAgent and/or queries to validate the information received. The extent of PII collected by this means depends on the individual's cooperation with investigators and between law enforcement agencies.

Privacy Risk: There is a risk that information collected by USSS from public sources, particularly social media, may be inaccurate.

Mitigation: USSS uses investigative and analytic techniques that focus on the review of data in order to verify its accuracy. Trained USSS personnel review all information collected from public sources to determine whether the information is pertinent and will further the Secret Service's mission. USSS will compare data collected from public sources against information from other sources, including official systems, in order to verify its accuracy. Any information collected that is not needed to carry out the Agency's mission or that cannot be verified as accurate from an official source is discarded.

Uses of the Information

There are no changes in the uses of the information. The PII transmitted using eAgent supports the Secret Service in accomplishing its investigative and protective mission. The eAgent system assists Secret Service employees in conducting searches to obtain protective and criminal intelligence information and determine if the subject(s) or activity has been encountered previously. Real-time or on-the-spot feedback may be provided to the field units if deemed necessary to support USSS mission requirements. The PII stored in the eAgent MART database is used for audit and quality control purposes.

Notice

The DHS/USSS-001 Criminal Investigation Information SORN[6] and DHS/USSS-004 Protection Information System SORN,[7] as well as this PIA, provide notice regarding the collection of information and the routine uses associated with the collection of the information. In some instances, it is not possible to provide notice to individuals prior to the collection of information as such notice could impede law enforcement investigations and checks in furtherance of the USSS protective mission. Individuals have no opportunity to consent, decline, or opt out of the project because of the law enforcement purposes for which the information was collected.

Privacy Risk: There is a risk that individuals who are subjects of an investigation may not know that information about them is being collected and maintained.

Mitigation: This risk is partially mitigated. Notice is provided through the DHS/USSS-001 Criminal Investigation Information System and DHS/USSS-004 Protection Information System SORNs and through publishing this PIA, including notice of the purpose of collection, redress procedures, and the routine uses associated with the collection of the information that USSS inputs and accesses using eAgent. Advanced notice of the collection of information to investigative targets or others involved in the investigation generally is not provided because it would compromise ongoing law enforcement investigations.

Data Retention by the project

There are no changes to the data retention requirements. Oversight and compliance records contained in or based upon eAgent's transaction archive are used to facilitate quality assurance reviews and reports, compliance reviews, and data measuring or estimating impact and compliance as it relates to adherence to applicable IT policies, directives, and operating standards (for example, certification and accreditation of equipment; operating system/software change management). The MART logs contain all information queried, which is retained for the purpose of FBI audits, internal (USSS) investigations, and for record retention. These IT management logs are destroyed or deleted when 3 years old or 1 year after it is determined that there are no unresolved issues relating to system stability or operation, software patching, and maintenance, etc., whichever is longer.

Information Sharing

Any information maintained in eAgent may be shared in accordance with the purposes and routine uses specified in the DHS/USSS-001 Criminal Investigative Information System and DHS/USSS-004 Protection Information System SORNs. To the extent that information may be

[6] *See* DHS/USSS-001 Criminal Investigation Information SORN, 76 FR 49497 (August 10, 2011), *available at* http://www.gpo.gov/fdsys/pkg/FR-2011-08-10/html/2011-20226.htm.

[7] *See* DHS/USSS-004 Protection Information Systems SORN, 76 FR 66940 (October 28, 2011), *available at* http://www.gpo.gov/fdsys/pkg/FR-2011-10-28/html/2011-27883.htm.

released pursuant to any routine uses, such release is made only if it is compatible with the purposes of the original collection, as determined on a case-by-case basis. For example, investigation information may be routinely shared with the Department of Justice (DOJ) for prosecution or other law enforcement purposes. PII that is a part of an investigative or criminal case file may be shared on a need-to-know basis with federal, state, and local law enforcement agencies, other foreign and domestic government units, or private entities in accordance with the routine uses outlined in the applicable SORNs.

Privacy Risk: There is a risk that information will be shared inappropriately by an external agency, beyond those individuals and entities that have a need to know.

Mitigation: This risk is mitigated through the integration of administrative, technical, and physical security controls that protect PII against unauthorized disclosure. Disclosure may only be made by authorized Secret Service employees engaged in criminal investigation and protective activities who are trained in the use of eAgent. Authorized Secret Service users of eAgent may only share the data with recipients who have a need-to-know, as outlined in the Routine Use portion of the SORNs.

Redress

Access, redress, and correction have not changed with this update. Access requests should be directed to Communications Center, FOIA/PA Officer, 245 Murray Lane, SW, 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 Investigation Information and DHS/USSS-004 Protection Information System SORNs, the systems of records may be exempt from the Privacy Act’s access and amendment provisions; therefore, record access and amendment may not be available in all cases. To the extent that records are not exempt under these authorities, DHS will provide access to them. Individuals, regardless of citizenship or legal status, may also request access to their records under FOIA.

Auditing and Accountability

The eAgent system uses role-based access controls for users and system administrators through the eAgent Client Manager, a web-based user interface. Standard system users can query, review, enter, and update information for submission back to NCIC and Nlets. eAgent users cannot delete data from NCIC and databases that are connected to Nlets; they can only query or submit new information and/or corrections. Each user may be assigned Terminal Agency Coordinator (TAC) and Administrator user roles. The TAC role may create users, disable users, and reset passwords for users in his or her assigned group. The Administrator role is a system administrator, allowing user and device administration for the entire user base. Administrator users are also responsible for creating and assigning message key permissions. Additionally, all sent or received transactions are validated and logged in eAgent MART. These transactions are monitored by the

TAC. eAgent users follow standard operating procedures and written search protocols when conducting searches and transmitting information. ISD has policies and TACs in the field offices along with certification training required every two years to reinforce approved practices to protect PII data.

The eAgent system merely serves as an interface to other systems. Other agencies have access to NCIC and Nlets, so they may see the same data on those systems, but no other agencies will have access to the eAgent application.

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 on identifying, protecting, and safeguarding sensitive PII.

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. NCIC certification (every two years) is required to access the NCIC system.

Responsible Official

Latita Payne
Disclosure and Privacy Officer
U.S. Secret Service
Department of Homeland Security

Approval Signature

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

____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security