Privacy Impact Assessment
for the

eAgent

DHS/USSS/PIA-015

July 17, 2015

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

Reviewing Official
Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The United States Secret Service (USSS or Secret Service) procured the National Crime Information Center/National Law Enforcement Telecommunications System Web Access System ("eAgent" system) as a Commercial Off-the-Shelf (COTS) upgrade from its legacy mainframe systems to a web-based application in order to improve timeliness and reliability of message processing and access law enforcement records. The eAgent application is a more user-friendly way for the USSS to access the information within the National Crime Information Center (NCIC) and the International Justice and Public Safety Network ("Nlets"). The previous method was difficult to use and susceptible to long wait times, errors, and timeouts. The eAgent system provides direct access through a common point to NCIC and Nlets critical law enforcement systems. USSS conducted this Privacy Impact Assessment (PIA) because eAgent transmits and stores personally identifiable information (PII) on subjects of protective and law enforcement interest to the Secret Service.

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, USSS personnel use NCIC and Nlets data services, and eAgent facilitates timely access to these services. The eAgent system assists Secret Service personnel in performing record checks of USSS data against NCIC and Nlets. 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 registration, stolen vehicle, and wanted person queries simultaneously.

NCIC is a nationwide information system established by the Federal Bureau of Investigation (FBI) as a service to criminal justice agencies. A computerized index of information on crime and criminals of nationwide interest and a locator file for missing persons,[2] NCIC assists USSS by providing and maintaining a computerized filing system of accurate and timely documented criminal justice information. Nlets links local, state, and federal law enforcement agencies, selected international agencies, and a variety of strategic partners of Nlets. 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.[3]

---

[1] 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] *See* http://www.fbi.gov/about-us/cjis/ncic for more information about NCIC.

[3] *See* https://www.nlets.org/ for more information about Nlets (previously called the National Law Enforcement

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 under investigation; individuals who are the subject of a special security event check; 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 to indicate that the search for the subject is no longer active. A "cleared" status does not mean that the record is deleted from NCIC, but rather that the individual 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 and access and exchange information transmitted through the Nlets network to identify the encountered individuals, determine if they are wanted by other law enforcement agencies for any 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.

eAgent users 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 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.

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. 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.

Telecommunications System).

The eAgent system consists of two components: a Message Switch System (MSS) that interfaces with both NCIC and Nlets and an application that routes queries to NCIC and Nlets through a browser-based user interface, which is available via desktop or laptop on the USSS network. Each transaction sent to and from NCIC and Nlets is logged in the MART database, the 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 any information used to query as well as the modifications made to NCIC records.

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?

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

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

The DHS/USSS-001 Criminal Investigation Information[4] and DHS/USSS-004 Protection Information System[5] SORNs cover the PII used by USSS in eAgent.

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

Yes.

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

eAgent does not create any substantive records requiring an agency-specific records retention schedule because the system only serves as an interface to other systems. However, General Records Schedule-24, Information Technology Operations and Management Records, covers audit logs and other compliance-related documentation in eAgent.

[4] 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.
[5] 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.

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.

Information used by eAgent is not covered by the PRA.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

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

eAgent 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.

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

USSS collects information directly from individuals during the course of a law enforcement encounter, a background investigation, or a special security event check. USSS personnel then enter the information from the individual into eAgent. 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 and contact USSS to report suspected violations or for an NCIC hit confirmation. Information in eAgent MART is obtained from the responses to the queries made to the NCIC and Nlets systems.

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

No. However, note that commercially available data systems may be sources for some portion of the information contained in the databases that are connected to Nlets, but eAgent does not query, enter information, or use data from those systems. It only has direct access to the NCIC system.

2.4 Discuss how accuracy of the data is ensured.

USSS policy mandates that the ISD is the only USSS entity that enters USSS warrants to ensure the integrity and accuracy of information entered into NCIC to guarantee compliance with NCIC. ISD verifies the accuracy of the information submitted before uploading any information into the NCIC using eAgent applications. The field units investigate, research, and follow-up on reported information in order to resolve or provide further details about the situation, subject, or activity, as well as to ensure accuracy of the data being submitted. Collected data is routinely compared to existing records to ensure accurate information is maintained. An investigator may check information provided by an individual or data source against any other approved source of information (within or outside USSS) before the investigator uses the information to make decisions about an individual. For example, each warrant entered by an ISD agent or analyst is double-checked by another agent or analyst from ISD to ensure that cross-checks have been made and that record data match investigative report data.

Furthermore, 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, recent 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.

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: Secret Service agents and officers are trained to collect only the necessary and appropriate PII for investigative 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 observation of suspicious activity or an investigation by an officer of the Secret Service or referred to USSS. 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.

Section 3.0 Uses of the Information

The following questions require a clear description of eAgent's use of information.

3.1 Describe how and why the project uses 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.

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.

3.4 Privacy Impact Analysis: Related to the Uses of Information, describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.

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

Mitigation: The Secret Service mitigates this risk by implementing various security measures for eAgent. The eAgent system logs user activity, locks sessions after twenty minutes of inactivity, limits access to authorized individuals, prevents account access after three unsuccessful login attempts, and warns users that unauthorized, improper use or access to the system may result in disciplinary action as well as civil and criminal penalties. Additionally, all queries and information received are kept in the MART system log files for audit and quality control purposes. The logs are audited by the FBI annually because the FBI audits any and all systems that query NCIC.

The eAgent Message Switch controls access at the user and device levels. System administrators can create message key groups containing any combination of message keys containing authentication codes. One or more message key groups may be assigned to a user or device. When a user tries to send a message, the eAgent MSS ensures that both the user and device have permission to send the transaction. Message key groups may contain message keys enabling read, add, modify, and delete to any type of file.

Furthermore, all eAgent users complete annual agency mandated privacy and security training, which stresses the importance of appropriate and authorized use of PII in government systems. NCIC training and certification testing is also required for the use of the NCIC system.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

The DHS/USSS-001 Criminal Investigation Information and DHS/USSS-004 Protection Information System SORNs,[6] as well as this PIA, provide notice regarding the collection of

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

information and the routine uses associated with the collection of the information. It is not possible to provide notice to individuals prior to the collection of information as such notice could impede law enforcement investigations because the purpose of eAgent is to assist USSS with investigating crimes against the U.S. financial system.

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

Individuals have no opportunity to consent, decline, or opt out of the project because of the law enforcement purposes for which the information was collected.

4.3 Privacy Impact Analysis: Related to Notice

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: Notice is provided through the DHS/USSS-001 Criminal Investigation Information System and DHS/USSS-004 Protection Information System SORNs[7] 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.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

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

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.

28/html/2011-27883.htm.
[7] *Id.*

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a privacy risk that information will be retained for longer or shorter than that is required or necessary.

Mitigation: This risk is mitigated by providing proper records retention training to all system users and periodically auditing the system to ensure that user permissions and roles are being adequately enforced by the system. The information in eAgent will be retained for the timeframes outlined in Section 5.1, unless directed otherwise by a superseding authority (e.g., litigation freeze, court order).

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state, and local governments and private sector entities.

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Yes, 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.[8] 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.

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

Any information maintained in eAgent may be shared in accordance with the purposes and routine uses specified in the DHS/USSS-001 Criminal Investigation Information and DHS/USSS-004 Protection Information System SORNs.[9] To the extent that information may be 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.

[8] *Id.*
[9] *Id.*

6.3 Does the project place limitations on re-dissemination?

Yes. When authorized users log on eAgent, they 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 they should ensure to appropriately safeguard PII contained therein. USSS may share information with other entities who are not users of NCIC or Nlets to resolve issues related to system problems or malfunctions, as well as in litigation or use in an open investigation. Information is not shared unless covered by a routine use outlined in DHS/USSS-001 Criminal Investigation Information and DHS/USSS-004 Protection Information System SORNs.[10]

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

Agency policy requires users of the system to document the dissemination of information obtained from the system in their memorandum of record on the matter. In addition, all transactions performed using eAgent that includes sending or retrieving data are logged in the eAgent MART database for audit and quality control purposes.

6.5 Privacy Impact Analysis: Related to Information Sharing

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

Mitigation: To mitigate this risk, disclosure may be made only by authorized Secret Service employees engaged in criminal investigative or protective activities, and who are trained on the use of eAgent. Authorized Secret Service eAgent users may only share the data pursuant to routine uses specified in the DHS/USSS-001 Criminal Investigative Information System and DHS/USSS-004 Protection Information System SORNs.[11]

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

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

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

[10] *Id.*
[11] *Id.*

DHS/USSS-004 Protection Information System SORNs,[12] 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.

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

Individuals seeking to contest the content of a record may submit a request in writing to the USSS FOIA Officer, 245 Murray Drive SW, Building T-5, Washington, DC 20223. Individuals may seek amendment of information in their criminal history record by following the instructions for record access and amendment in the NCIC SORN.[13] However, as noted in 7.1, the systems of records may be exempt from the Privacy Act's amendment provisions; therefore, record amendment may not be available in all cases.

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

The mechanism for requesting correction of information is specified in the DHS/USSS-001 Criminal Investigation Information System and DHS/USSS-004 Protection Information System SORNs.[14] The Secretary of Homeland Security has exempted this system from the notification, access, and amendment procedures of the Privacy Act because it is a law enforcement system. However, DHS/USSS will consider individual requests to determine whether or not information may be released.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals may have limited access or ability to correct their information.

Mitigation: If any actions are taken against the individual as a result of, or in connection with, information requested or provided in the USSS-generated record, certain statutory or regulatory appeal rights or constitutional due process rights to access, amend, or otherwise challenge the information may exist. For example, if an individual is arrested as a result of the existence of an USSS-generated NCIC record indicating a criminal warrant exists, the individual may have statutory or constitutional rights to challenge the arrest and access information concerning the validity or basis for the warrant.

---

[12] *Id.*
[13] *See* DOJ/FBI-001National Crime Information Center (NCIC), 64 FR 52343 (September 28, 1999).
[14] 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 and 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.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

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

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 their 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.

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 on identifying, protecting, and safeguarding sensitive PII.

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

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?

The eAgent information system is a new interface for accessing the NCIC and Nlets, which USSS has already been accessing for years under current MOA agreements. Any future change in function, access to other systems, or third party access to eAgent would undergo the official approval process and appropriate privacy review.

Responsible Officials

Latita Payne
Disclosure and Privacy Officer
U.S. Secret Service

Approval Signature

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security