Privacy Impact Assessment
for the

eCASE Management System

DHS/USSS/PIA-019

July 12, 2017

Contact Point
Latita M. Payne
Privacy Officer
United States Secret Service
(202) 406-5838

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

Abstract

The United States Secret Service (USSS) Security Clearance Division's (SCD) Electronic Case Management System (eCASE) supports the tracking of applicant and non-applicant background investigation cases. Along with the Clearance, Logistics, Employees, Applicants, and Recruitment (CLEAR) system, which assists USSS employees in managing applicant data throughout the hiring processing, eCASE is part of a new boundary identified as the Human Capital Management System (HCMS). The Secret Service is conducting this privacy impact assessment (PIA) because eCASE collects personally identifiable information (PII) on members of the public.

Overview

USSS's SCD has a need to support the tracking of applicant and existing employee background investigations associated with job vacancies and employee reinvestigations. The tracking of individual investigations are maintained in eCASE to manage resource scheduling and the status of each investigation as it moves through various steps of validating information contained in employment artifacts. Investigators verify applicant information collected from employment sites like Monster and USAJobs, documents provided by the applicant such as Standard Form 86 (SF 86),[1] medical history based on eligibility requirements, and information contained in provided resumes. USSS downloads or prints information directly from the employment site to be stored in paper format and kept in paper case files restricted to SCD personnel and subsequently locked in a secure area. Only those with an absolute need-to-know may access the paper case files related to the applicant investigation process.

The USSS in-house developed eCASE tool is designed to assist SCD with initiating the validation and verification process based on information contained in the employment package. A person submitting an application is referred to as an "applicant." If the applicant meets the minimum job requirements, he or she is notified via email or U.S. Mail based on provided contact information he or she has been selected for employment contingent upon a successful security background investigation. When transitioning to the security background phase, the applicant is now known as a "candidate." The eCASE tool then generates a unique tracking ID number to manage the investigative process.

Designated SCD personnel input limited, but necessary information from the employment package to initiate an electronic case file on the candidate that remains linked with the individual if he or she passes the background investigation and accepts employment. The unique tracking ID number that uniquely identifies the person and signifies the investigating office is permanently

[1] See SF-86 Questionnaire for National Security Positions, available at https://www.opm.gov/forms/pdf_fill/sf86-non508.pdf.

assigned to the candidate. Each phase of the candidate validation process is denoted in eCASE as pass or fail. Phases of the validation process conducted by SCD include credit check, criminal history, employment history, military duty, education verification, and candidate interviews.

Information voluntarily provided in the employment submission package include the resume, SF 86, credit reports, military personnel record, and educational transcripts validated against public and private records sources such as Lexis Nexis and the National Crime Information Center (NCIC) database maintained by the Federal Bureau of Investigations (FBI). Once in the eCASE tool, a new randomly generated three digit number is created that represents the type of case being investigated. This allows various departments within the USSS engaged in the validation process to track the status of individual investigations. eCASE maintains two case types: initial background check and reinvestigations check. SCD reinvestigates USSS employees who have a Top Secret Personnel Clearance every five years to ensure employees do not pose a risk to the operational mission of USSS or to national security. Investigators check for changes in marital status, credit checks for signs of financial stress, changes in education, and updated criminal checks.

USSS manually enters the limited PII on the candidate into the eCASE tool: name, case number, case establishment date, date of birth, gender, Social Security number (SSN), place of birth, home address, eye color, height, weight, and citizenship; no additional information can be added or modified in the fields. Additionally, the eCASE tool does not allow the investigator to upload artifacts into the system. Instead, USSS maintains all information related to the investigative phase of the hiring process or employee reinvestigation process in paper records with original artifacts sent to USSS headquarters for inclusion in paper case files. USSS depends on manual case files, yet are in the process of developing electronic tools wherever possible to reduce paper dependency.

The eCASE and the Clearance, Logistics, Employees, Applicants and Recruitment (CLEAR) system make up the new Human Capital Management System (HCMS) boundary. CLEAR assists USSS employees in managing applicant data throughout the hiring processing and is further discussed in a privacy impact assessment (PIA)[2].

[2] *See* DHS/USSS/PIA-013 Clearances, Logistics, Employees, Applicants, and Recruitment (CLEAR), *available at* www.dhs.gov/privacy.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The collection of information is authorized by 5 U.S.C. § 1104; Executive Order 9397 (as amended); 18 U.S.C. §§ 3056 and 3056A; 5 U.S.C. § 9101; and 5 C.F.R. Chapter 1, Subchapter B, Parts 731, 732 and 736.

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

The following SORNs cover the collection, maintenance, and use of the information contained in eCASE:

- Non-Criminal Investigation Information System[3] covers information related to applicants for employment or current employees of the USSS or other federal or state entities who have taken a polygraph;
- Recruiting, Examining, and Placement Records[4] covers records used in considering individuals who have applied for positions in the federal service by making determinations of qualifications; and
- Personnel Security Management System[5] covers records of personnel security-related clearance actions, to record suitability determinations, to record whether security clearances are issued or denied, and to verify eligibility for access to classified information or assignment to a sensitive position.

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

Yes. The eCASE tool has completed the accreditation process; the ATO is expected to be granted pending approval of the Privacy Impact Assessment (PIA).

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

Yes. General Records Schedule (GRS) 18, Security and Protective Services Records, covers Personnel Security Clearance Files under item 22. Disposition of routine recruitment files such as those contained in the eCASE are governed by the Office of Personnel Management

[3] DHS/USSS-003 Non-Criminal Investigation Information System SORN, 76 FR 66937 (October 28, 2011).
[4] OPM/GOVT-5 Recruiting, Examining, and Placement Records SORN, 79 FR 16834 (March 26, 2014).
[5] DHS/ALL-023 Personnel Security Management System SORN, 75 FR 8088 (February 23, 2010).

guidance in Delegated Examining Operations Handbook, Appendix C, Records Retention and Disposition Schedule and the National Archives and Records Administration's GRS 1, Civilian Personnel Records, items 3 and 33b. (Note: A new GRS 2.1 covering "Employee Acquisition Records" is pending final NARA issuance, at which time it will become a definitive authority or citation for many of these record types).

Records in eCASE are maintained solely for tracking a candidate throughout the clearance process until accepted or rejected for USSS employment. Exceptions may occur when records are retained to support procedural or legal challenges related to the clearance or hiring process (*i.e.*, when the USSS is barred from removing records related to hiring or background information due to pending legal challenges, discovery motions, judicial "hold" others).

Employee data for periodic reinvestigations is destroyed upon notification of death, or no later than 5 years after separation or transfer of employee (or termination of the applicant relationship) whichever is later. (GRS 18, item 22a).

Disposition of other investigative records contained within eCASE are governed by retention periods which correspond to the specific case type developed (*e.g.*, 30 years for judicial criminal cases, 10 years for non-judicial criminal cases, and 5 years for non-criminal case). Case files involving crimes that have no statute of limitations (*e.g.*, murder) 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. Relevant retention schedule numbers are N1-087-89-002 and N1-087-92-002. However, a new DHS Enterprise Schedule designed to standardize retention of investigative records across the Department and its Components is currently pending review by the National Archives and Records Administration that may change some of the retention periods once it is approved and issued.

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 provided by an applicant via forms in the SF 86 suite (OMB Control Number 3206-0005) or its electronic equivalent (such as E-QIP) provides the foundational data collected by eCase. As noted in the Overview, when an applicant is cleared for processing as a "candidate," he or she is no longer treated as a member of the "general public" and information collected under an investigative function is not subject to provisions of 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.

The eCASE tool contains information manually inserted by SCD personnel on candidates for federal employment and existing employees going through the reinvestigation process. The information includes:

- Case number;
- Case Title;
- Case Type;
- Controlling Office;
- Case status open/close date;
- First and last name;
- Last four numbers of SSN;
- Employment and all education histories;
- Applicant contact information;
- Marital status;
- Physical results (recorded Pass/Fail); and
- Polygraph results (Pass/Fail, and polygrapher comments).

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

SMD collects and maintains information provided by the applicant in his or her SF-86 questionnaire, military medical records, educational transcripts, credit history, tax records, and employment application in paper case files. Using this information, investigators will conduct background checks using written consent provided by the applicant against public records and government agencies systems such as Internal Revenue Service (IRS), FBI, and Department of Defense (DoD). Additional information may be gathered and included in the paper case file such as notes from the investigator, eye exam results provided by the applicant, and the results of the polygraph assessments as required by the nature of the position. Any artifacts derived from

the investigative process are kept in paper case files and are collected with the applicant's consent. SF-86 questionnaire has consent requirements within the document.

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

Yes. The Office of Investigations (INV-SP) may use credit reporting information as well as Lexis/Nexis during the background investigation process.[6] USSS verifies information collected from the applicant against publicly available, commercially available, or government databases based on information provided by the applicant or employee.

2.4 Discuss how accuracy of the data is ensured.

USSS verifies information obtained directly from applicants as part of the USSS background investigation process. Investigators may interview references provided by the applicant. There are also cross checks against information that is available from government databases (such as tax returns or criminal history checks) and commercial databases (such as credit history checks). Inconsistencies are resolved in interviews with the applicant. USSS cannot verify the accuracy of information in public databases such as credit bureaus, criminal databases, or IRS. Any discrepancies or derogative information is brought to the applicant's attention for the applicant to correct with the public agencies.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that inaccurate information could negatively impact a candidate's selection for a position.

Mitigation: This risk is mitigated through USSS's implementation of 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 necessary to be offered employment. Additionally, USSS personnel collect information using carefully defined parameters, specifically tailored to identify relevant information for official purposes, while also minimizing false positives (*i.e.*, mis-hits or information unrelated to the Secret Service's mission). Any information collected that is not needed to carry out the Agency's mission is discarded.

Information collected from the applicant is verified against publicly available, commercially available, or government databases. Candidate-designated references are also

[6] For a detailed description of the personnel security process at DHS, *see* DHS/ALL/PIA-038 Integrated Security Management System (ISMS), *available at* www.dhs.gov/privacy.

interviewed as part of the review process. At the conclusion of the review process, USSS interviews the candidate and he or she is given the opportunity to address any items of concern. An appeals process is in place as a further check against inaccuracies. The appeals process consists of the applicant providing supplemental background information to adjudicators in order to mitigate any security concerns. For example, a requirement for obtaining a Top Secret Security Clearance is to maintain financial stability. If derogatory or questionable information is reported by creditors, the applicant will have an opportunity to mitigate the concern by submitting documentation showing corrective action. All appeal information is submitted directly to the Chief of the Security Clearance Division for a final adjudication.

Privacy Risk: There is a risk that eCASE could collect more PII than is necessary to accomplish its mission.

Mitigation: Similarly, this risk is mitigated through USSS's implementation of investigative and analytic techniques that focus on the review of data in order to verify its accuracy and relevance. Trained USSS personnel review all information collected from public sources to determine whether the information is pertinent and necessary to the underlying case. Additionally, USSS personnel collect information using carefully defined parameters, specifically tailored to identify relevant information for official purposes, while also minimizing false positives (*i.e.*, mis-hits or information unrelated to the Secret Service's mission). Any information collected that is not needed to carry out the Agency's mission is discarded.

Section 3.0 Uses of the Information

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

3.1 Describe how and why the project uses the information.

USSS uses all information collected to determine the suitability of the applicant to the relevant vacancy and tracks the process through the eCASE tool. USSS uses PII to facilitate the background investigation phase of the hiring process. Background checks are either pass or fail with a clearance ultimately being granted or not. Additionally, medical physical results as provided by the applicant from the physician or doctor, if applicable, are recorded as a pass or fail. Aggregated statistics may be provided for congressional reporting or for a Freedom of Information Act (FOIA) request.

USSS retains the results of internal management assessments. Internal management assessments are evaluations of the candidate's relevant employment or education experiences, as well as ratings from the candidate interviews.

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. eCASE is not used to discover predictive patterns or anomalies.

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

No. eCASE is an internal tool developed to track steps with the candidate hiring and reinvestigation process.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a privacy risk that authorized users could gain access to and use eCASE data for purposes inconsistent with the original collection.

Mitigation: To mitigate this risk, strict need-to-know and least privilege restrictions are considered when granting access to eCASE. Further, the most sensitive information in an applicant case file is only accessible by designated personnel in the SCD and is not available to other personnel.

All users undergo training on handling privacy sensitive information each year. eCASE collects information that is strictly necessary for completing and tracking the background investigation process for applicants and existing employees.

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.

In addition to this PIA, DHS/USSS-001 Non-Criminal Investigation Information System, OPM/GOVT-005 Recruiting, Examining, and Placement Records, and DHS/ALL-023 Personnel Security Management System provide notice regarding the collection of information and the routine uses associated with eCASE. Further, the SF 86 forms completed by applicants prior to background investigations have a Privacy Act Statement, notifying them of the intended usage of information collected and ramifications of not providing the requested information.

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

Applicants are given the opportunity to decline to provide their own information by not submitting their information for the employment opportunity. Declining to provide their information simply means that the individual chooses not to participate in the hiring process for the employment opportunity.

The SF-86 questionnaire has a written consent to uses built in to the document. Specifically, any information provided on the form, and information collected during the investigation, may be further disclosed without the candidate's consent by an agency maintaining the information in a system of records as permitted by the Privacy Act, and by routine uses, a list of which are published by the agency in the Federal Register.[7] USSS is required to provide the candidate with a copy of its routine uses.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a privacy risk that applicants will not receive adequate notice detailing the purpose for the collection of their information, as well as its use, maintenance, and dissemination.

Mitigation: USSS partially mitigates this privacy risk by providing notice to applicants and candidates through publishing this PIA and the associated SORNs. Additionally, a Privacy Notice is provided to the applicants at the time they submit their information through USAJOBS.gov website or the benefit forms process completed by the applicant for background investigations and security clearance checks. By providing notice when collecting information, USSS mitigates the privacy risks associated with notice, including the lack of understanding on the part of the individuals regarding the collection and use of their PII, their right to refuse to participate in the information collection, and their ability to correct inaccurate information. Applicants are given the opportunity to decline to provide their own information by not submitting their information for the employment opportunity. Declining to provide their information simply means the individual chooses not to participate in the hiring process. There is no written consent required since the applicant has already consented by applying for the job. There is no guarantee of employment because the position requires a successfully adjudicated background investigation.

The SF-86 questionnaire submitted with the application package provides the candidate for employment the opportunity to provide written consent to allow the candidates information to be used for specified additional purposes other than employment. The form also allows for certain other agencies to verify sensitive date the applicant provided. Information provided on the form may be used to verify information collected during the background investigation and shared with

[7] 5 U.S.C. 552a(b)(3).

additional agencies such as the FBI, without the candidate's explicit consent. USSS maintains the information collected on the SF-86 questionnaire in a system of records as permitted by the Privacy Act. USSS provides the candidate with a copy of the potential uses of that candidate's information by applying for the available positon.

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.

It is the policy of the Secret Service to create or retain records associated with applicants and candidates only when necessary and for the minimum amount of time needed to successfully execute the human resources and associated security functions of our agency, and to comply with applicable regulations.

To this end, the Secret Service has explicitly adopted the retention protocols outlined by Office of Personnel Management (OPM) and promulgated in the GRS of the NARA. These schedules are "media neutral," and apply to both paper records, as well as electronic records such as those contained in IT systems, databases, and scanned or digitized files. As part of a recent NARA effort to update, expand, and reorganize the GRS, new guidance for managing Employee Acquisition Records has been developed and is pending final release under GRS 2.1. Likewise, a new GRS 5.6 covering Security Records will govern security clearance investigation records. Until then, controlling provisions of the legacy GRS 1 and GRS 18 govern data retention as follows:

- Records for those applicants who are rejected for a position (or who reject further processing by withdrawing from consideration) during the Suitability Determination process (before a formal background investigation is opened) are to be held for 2 years after the corresponding vacancy case file is closed, then destroyed. (See GRS 1, Item 5).
- Records for those candidates who are rejected (or who reject further processing by withdrawing from consideration) after a formal Background Investigation case is opened are to be held until notification of death or not later than 5 years after the termination of the applicant relationship, whichever is applicable, then destroyed. (See GRS 18, Item 22).

Records for applicants or candidates who successful enter the agency as employees (along with any subsequent data for periodic reinvestigations) is destroyed upon notification of death, or no later than 5 years after separation or transfer of employee whichever is later. (GRS 18, item 22a].

Disposition of other investigative records contained within eCASE are governed by retention periods that correspond to the specific case type developed (*e.g.*, 30 years for judicial criminal cases, 10 years for non-judicial criminal cases, and 5 years for non-criminal case). Case files involving crimes that have no statute of limitations (*e.g.*, murder) 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. Relevant retention schedule numbers are: N1-087-89-002 and N1-087-92-002. However, a new DHS Enterprise Schedule designed to standardize retention of investigative records across the Department and its Components is currently pending review by the National Archives and Records Administration that may change some of the retention periods once it is approved and issued. For example, judicial criminal cases have been proposed for a reduction in retention, from 30 years to 20 years.

Exceptions to these protocols may occur when records are retained to support procedural or legal challenges related to the clearance or hiring process (*i.e.*, when the USSS is barred from removing records related to hiring or background information due to pending legal challenges, discovery motions, judicial "hold" orders).

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a privacy risk that eCASE will retain information for a period longer than necessary to achieve its mission objectives.

Mitigation: Although there is always an inherent risk with retaining data for any length of time, data retention periods for the associated system are consistent with the concept of retaining information in eCASE in accordance with the approved NARA retention schedules, as outlined in Section 5.1.

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 government, 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.

No. USSS does not have any interconnection with nor does it share information electronically with outside systems. SCD does, however, manually enter the individual's case

number into the OPM's Personnel Investigations Processing System (PIPS)[8] for tracking purposes. Prior to being entered into the eCASE tool, minimally necessary information will be used to validate information with other agencies such as IRS, FBI, and DoD to conduct background investigations or validate information provided by the applicant. For example, USSS will use names and date of birth to facilitate criminal background checks and military service, and SSNs to facilitate checks of state and federal tax records.

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

eCASE does not share information outside of DHS. However, USSS shares information collected, maintained, used, and disseminated during the hiring process consistent with routine uses in the applicable SORNs. This information does not come from eCASE.

6.3 Does the project place limitations on re-dissemination?

No.

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

eCASE does not share information outside of DHS. SCD manually enters the candidates' case number into OPM's PIPS for tracking purposes. USSS documents the disclosure in the candidates' paper case file when the candidates' case number is disclosed to OPM's PIPS.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that information will be shared outside of USSS for the purpose inconsistent with applicable SORNs.

Mitigation: All information collected, maintained, used, and disseminated by USSS during the hiring process is covered by the Privacy Act. Information may only be disseminated consistent with the routine uses in applicable SORNs. USSS does not share information externally in a manner inconsistent with these Privacy Act protections. Information shared in accordance with routine uses of applicable SORNs is reviewed by the USSS Privacy Officer, Office of Chief Counsel, or the Office of Investigation Support Services prior to release.

[8] *See* OPM PIA's *available at* https://www.opm.gov/information-management/privacy-policy/#url=Privacy-Impact-Assessments.

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?

The Secretary has exempted the eCASE system from certain provisions of the Privacy Act, as reflected in DHS/USSS-003 Non-Criminal Investigative Information System SORN in order to prevent harm to law enforcement investigations or interests. However, access requests will be considered on a case-by-case basis if made in writing to the Secret Service's FOIA Officer, Communications Center (FOIA/PA), 245 Murray Lane, Building T-5, Washington, D.C. 20223, as specified in the Non-Criminal Investigative Information System SORN. An applicant not selected for employment or advancement is notified in writing and similarly may file a FOIA request to gain access to their information, which will be considered on a case-by-case basis.

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

Relevant information uncovered during the background check process is discussed with the candidate by the investigator during the interview process. The candidate will have the opportunity to discuss any discrepancies and provide evidence to correct any errors.

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

Information collected is provided by the applicant/candidate and compared against public, government, or private sources. Any discrepancies identified are communicated to the candidate for clarification and correction during the interview process.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a privacy risk that information stored on applicants is not accurate, and hiring decisions are made based on the incorrect information.

Mitigation: Investigators make every effort to ensure that accurate information is obtained from the applicant and his or her references. This information is confirmed in interviews with applicants.

Further, redress is available through written request to the Secret Service's FOIA Officer as described above; however, providing an individual access or correction of the records may be limited for law enforcement reasons as expressly permitted by the Privacy Act.

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?

Only personnel with a direct need to either create or use the data in eCASE are granted access to the system. The most sensitive areas of the system are only made available to personnel with a direct need-to-know in the Security Clearance Division. All users are trained on handling and the use of PII.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All Secret Service employees are required to receive annual privacy and security training to ensure their understanding of proper handling and securing of PII. DHS has published the "Handbook for Safeguarding Sensitive PII," providing employees and contractors additional guidance.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

DHS physical and information security policies dictate who may access USSS computers and filing systems. Specifically, DHS Management Directive 4300A outlines information technology procedures for granting access to USSS computers. Access to the information is strictly limited by access controls to those who required it for completion of their official duties.

Users granted access to eCASE must receive authorization from the Chief of the Security Clearance Division, or the Chief's delegated representative. Authorized users are then added to predefined functional role with defined permissions through Active Directory. Authorized personnel access the eCASE tool from their desktop web browser, where access into specific file containers is controlled and monitored once authenticated into the system. Contractor access is limited to the application development team with general contractor access prohibited. Access control into the eCASE application is controlled by the Enterprise Microsoft Active Directory database, which provides eCASE with lookup capabilities to the Enterprise Person (ePerson)[9] system for attribute information such as office location, phone number, and organizational assignment. The eCASE database is provided and maintained by the Application Provisioning System (APS) General Support

[9] *See* DHS/USSS/PIA-016 Enterprise Person System, *available at* https://www.dhs.gov/privacy.

System (GSS).

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?

There are currently no sharing agreements or MOUs with any outside component of DHS or outside government agency. USSS regards the information within eCASE and the processes that generate it to be sensitive and for internal use only. Any new uses of information shall be reviewed by the USSS Privacy Officer, Office of Chief Counsel, and the respective program office.

Responsible Officials

Latita Payne
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