Privacy Impact Assessment
for the

Applicant Lifecycle Information System (ALIS)

DHS/USSS/PIA-023

August 21, 2018

Contact Point
Christal Bramson
Acting Privacy Officer
United States Secret Service
(202) 406-5838

Reviewing Official
Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The United States Secret Service (USSS) Office of Human Resources (HUM) uses the Applicant Lifecycle Information System (ALIS) to support the hiring process for USSS Special Agents (SA), Uniform Division (UD) Officers, and Administrative, Professional, Technical (APT) personnel. ALIS is a new system that will replace the Clearances, Logistics, Employees, Applicants, and Recruitment (CLEAR) application component of the USSS Human Capital Management System (HCMS). The USSS is conducting this privacy impact assessment (PIA) because ALIS collects personally identifiable information (PII) from current USSS employees and members of the public.

Overview

ALIS is a new applicant tracking system used by the USSS Office of Human Resources (HUM), including the Security Management Division (SMD), Talent & Employee Acquisition Management Division (TAD), Safety, Health, and Environmental Programs Division (SAF), and by USSS Field Offices. ALIS replaces the CLEAR application component of the USSS HCMS.[1] USSS decommissioned the CLEAR application. USSS uses ALIS to process all new USSS applicant data.

TAD personnel manage the hiring process of an applicant within ALIS. This process includes a review of the applicant's application materials; an initial National Crime Information Center (NCIC) check; an entrance examination (if applicable); a Special Agent and Uniformed Division Pre-Employment Review (SUPER) interview (if applicable); and a conditional job offer, if the applicant is selected. Members of SMD manage the security investigation of an applicant who is initially selected (i.e., given a conditional job offer). This process includes a security interview, a polygraph examination, a medical examination, a drug test, and a background investigation.[2] For those applicants whose positions require them, the medical examination and drug test stages are usually processed by SAF. The progress of these steps are recorded in ALIS and tracked from beginning to end to support the hiring process. ALIS does not generate data in and of itself, rather the only unique information reflected in the systems pertains to whether an applicant passes or fails a specific stage of the hiring process.

Access to ALIS is limited to system administrators/developers and certain members of TAD, HUM, SMD, SAF, and USSS Field Offices who require access to perform their functions in the hiring process. TAD is the main user of ALIS, and provides oversight to ensure applications

[1] The HCMS was comprised of two applications: CLEAR and eCase. These are legacy applications that were previously used to manage and process USSS employment applications throughout the hiring process. Upon publication of the ALIS PIA, DHS will retire the CLEAR PIA. The eCase application has been added as a subsystem to the ePerson major application.

[2] As with the hiring stages managed by TAD, some of these stages do not apply to applicants for all USSS positions.

are processed efficiently. The other offices that have access use ALIS to import relevant documentation, update an assigned hiring stage to indicate if they have received required documents, and to indicate if an applicant can proceed to a subsequent stage in the hiring process. A separate username and password is not required for access to ALIS; users are automatically logged into the application upon accessing its URL through the user's Secret Security Network (SSNet) authorization. A user's access is restricted within the ALIS application by role-based access control to only the specific data and consoles to which he or she has been approved to access. A user's network account is added to the Active Directory group that is applicable to the user's role within the ALIS application.

ALIS serves as a repository for all applicant forms and documents except the medical or drug test-related documents, which are retained within the Safety, Health, and Environmental Programs Division. In order to access job applicant data and background investigation information, ALIS uses the following data acquisition processes:

Department of Treasury/Monster Government Solutions (MGS)–Career Connector

MGS–Career Connector hosts the USAJOBS website[3] that allows prospective applicants to submit their applications for advertised USSS SA and UD vacancies. USSS TAD personnel log in to Career Connector (a component of the Treasury/MGS) to screen and identify potentially qualified applicants. TAD personnel screen applicants via position-specific questionnaires submitted through Career Connector. An algorithm within the Career Connector application identifies "qualified" applicants based on their responses to the questionnaire.[4]

On a daily basis, TAD personnel run a report in Career Connector to pull the data of qualified applicants. The file is then downloaded and placed on a secure USSS file server by TAD personnel. Within the USSS Application Provisioning System (APS) boundary, an Informatica Server (a data extraction, transformation, and loading tool) pulls the Career Connector data from the secure file server and formats it into Extensible Markup Language (XML) format. The XML formatted data provides a flexible text format for mapping applicant data from the Informatica server to the production ALIS Oracle database. All applicant information ends up in ALIS.

Office of Personnel Management (OPM)–Electronic Questionnaires for Investigations Processing (e-QIP)

To support the background investigation and clearance process for applicants who have been sent a Conditional Offer Letter, TAD/HUM personnel log into the OPM e-QIP application in

[3] USAJOBS.gov is the federal government's website for posting civil service job opportunities with federal agencies. The site is operated by the OPM. For additional information, *see* https://www.opm.gov/information-management/privacy-policy/privacy-policy/usas-pia.pdf.

[4] Qualification standards are minimum requirements for a position, and most permit an applicant to qualify based on education, experience, or a combination of the two.

order to generate a request (which includes e-QIP login credentials) for an applicant to fill out the Questionnaire for National Security Positions (SF-86). The request is then automatically emailed to the applicant by the OPM e-QIP system.[5] Once the SF-86 is submitted in e-QIP by the applicant, an encrypted email (with an attached .PDF applicant file) is sent to the EQIP.USSS@usss.dhs.gov email account. The USSS e-QIP service (configured within the Informatica Server) checks the email account for new mail and copies the attached files to the e-QIP Oracle staging server within the APS Data Services Oracle cluster. The Informatica Server decrypts the data using the private key and loads the record into the ALIS database server under the e-QIP case/request number.

USSS Enterprise Person (ePerson)

ALIS also interfaces with the USSS ePerson[6] database for look-up capabilities to review USSS employee attribute information, such as employee name, office code (e.g., HUM, CIO), and office location (i.e., country), for ALIS users. This connection is used to identify current USSS personnel who are reviewing applicants within ALIS.

Manually Uploaded Documents

TAD personnel will manually upload various documents into ALIS during the hiring process, including the UD SUPER interview rating form (Secret Service Form 4368), the SA SUPER interview rating form (SSF 4367), and the UD/SA applicant acknowledgement/nondisclosure agreement form (SSF 4369). SMD personnel also manually upload documents related to the applicant's background investigation, including: a working copy of the SF-86, background reports from the field offices, written statements (if applicable), amended applicant forms (if applicable), polygraph report(s), credit reporting information, military medical records, educational transcripts, tax records, and employment application.

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 (Delegation of Authority for Personnel Management); Executive Order 9397 *Numbering System For Federal Accounts Relating to Individual Persons*, as amended by Executive Order 13478; 5 U.S.C. § 9101 (Access to Criminal History Records for National Security and Other Purposes); and 5 C.F.R. Chapter 1, Subchapter B, Parts 731, 732, and 736.

[5] For more information *see* https://www.opm.gov/information-management/privacy-policy/privacy-policy/eqip.pdf.
[6] ePerson is the USSS personnel system. *See* DHS/USSS/PIA-016 Enterprise Person (ePerson) System, *available at* https://www.dhs.gov/publication/dhsussspia-016-enterprise-person-system.

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 ALIS:

- Non-Criminal Investigation Information System[7] covers information related to applicants for employment or current employees of the USSS or other federal or state entities who have taken a polygraph examination;
- Recruiting, Examining, and Placement Records[8] 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[9] 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. ALIS in the process of completing its Authority to Operate (ATO) certification, which includes a system Security Plan. An ATO is expected to be granted pending approval of this PIA.

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

Yes. Disposition of routine recruitment files such as those contained in the ALIS are governed by National Archives and Records Administration (NARA) General Schedule 2.1, "Employee Acquisition Records," and well as OPM guidance in the Delegated Examining Operations Handbook, Appendix C, Records Retention and Disposition Schedule. Employee management administrative records will be destroyed when three years old, in accordance with General Records Schedule (GRS) 2.2, item 010. Job vacancy case files will be destroyed when two years old, in accordance with GRS 2.1, items 050 and 051.

For retention and disposition purposes, personnel security and access clearance records of rejected employees are divided into two categories:

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

- 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 held for 2 years after the corresponding vacancy case file is closed, then destroyed. (See GRS 2.1, Item 50.)
- Records for those applicants 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 5.6, Item 180.)

If an applicant becomes a USSS employee, the information becomes part of their personnel records, subject to the retention policy of the ePerson system. Applicant tracking data will be destroyed or deleted when three years old, according to GRS 4.1, item 010, and vacancy tracking data will be destroyed or deleted when two years old, according to GRS 4.1, item 010.

Records in ALIS are maintained solely for tracking an applicant throughout the hiring process until he or she is accepted or rejected for USSS employment. Exceptions to retention schedules may occur when records are retained to support procedural or legal challenges related to the hiring process (e.g., when the USSS is subject to a litigation hold due to a pending legal challenge).

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 is collected using the OPM form SF-86, which is under OMB No. 3206-0005.

Section 2.0 Characterization of the Information

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

The following information is collected and retained concerning job applicants (members of the public) within ALIS:

- Full name;
- Date of birth;
- Place of birth;

- Social Security number (SSN); and
- Applicant phone number and email address.

The following information is collected on the SF-86 and retained for job applicants (members of the public) in ALIS:

- Other names used;
- Race;
- Gender;
- Sex;
- Other physically descriptive information, such as height and weight;
- Citizenship;
- Education history;
- Employment history;
- Residential history;
- Military service;
- Marital status;
- Relatives' full name;
- Relatives' date of birth;
- Relatives' place of birth;
- Relatives' contact information;
- Foreign travel and activities;
- Psychological and emotional health treatment;
- Police record;
- Drug usage;
- Financial information (to include delinquent debts, bankruptcies, misuse of corporate funds, liens, repossessions, and wage garnishments); and
- Contact information of personal and professional references.

The following information is collected and retained for job applicants (members of the public) during the Security Interview Stage within ALIS:

- Physical assessment results (recorded Pass/Fail);
- Polygraph results (Pass/Fail and examiner comments);
- Drug test results;
- Psychological assessment results;
- Results from criminal background checks;
- Credit report;
- Military medical records;
- Educational transcripts;
- Tax records;
- Employment application;
- Investigation notes; and
- Eye exam results.

The following information is collected and retained about current USSS personnel and is displayed on various user interfaces within ALIS to identify the personnel to which an applicant's hiring stage has been assigned:

- First and last name;
- Duty location (country); and
- Office code.

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

Initial applicant data from Career Connector is imported into the ALIS database in order to build the applicant's profile within ALIS. Information the applicant provides in his or her eQIP SF-86 Questionnaire, military medical records, educational transcripts, tax records, and employment application is also uploaded and retained within ALIS. Additional information may be uploaded to the applicant's profile, such as notes from the investigator, eye exam results provided by the applicant, and the results of the polygraph examination, if applicable. Any artifacts derived from the investigative process are uploaded and retained within ALIS.

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

USSS personnel may use credit reporting information as well as LexisNexis during the background investigation process. Information collected from the applicant is verified against publicly available, commercially available, or government databases based on information provided by the applicant.

2.4 Discuss how accuracy of the data is ensured.

Information obtained directly from applicants is verified as part of the USSS background investigation process. As a required part of the process, investigators interview references provided by the applicant, as well as any additional references developed during the course of the background investigation in order to verify applicant-submitted information. 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.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a privacy risk associated with the volume and sensitivity of the personal information maintained in ALIS.

Mitigation: This risk is mitigated by role-based access to ALIS. Working under the least-privilege principle, applicant data can be accessed only by individuals that require the information to perform their specific job function in support of the hiring process. The USSS only collects the necessary data needed to complete the hiring process. Medical or drug test-related documents are retained by SAF and manually removed by administrators after the retention period ends. No information beyond non-identifying statistical information is routinely shared externally. In the event that a congressional inquiry is made in regards to an ALIS record, the Secret Service Congressional Affairs Program (CAF), located within the Office of Intergovernmental and Legislative Affairs (ILA), would respond to Congressional inquiries, requests, and correspondence. Any congressional inquiries that may contain PII are tracked via the DHS Executive Secretary (Execsec) Router, although such inquiries are rare.

Privacy Risk: There is a risk that inaccurate information could negatively impact an applicant's selection process.

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 an offer of 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. Applicant designated references are also interviewed as part of the review process. At the conclusion of this process, the applicant is interviewed and able to address any items of concern. An appeals process for challenging security clearance determinations is in place as a further check against inaccuracies. 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 Management Division for a final adjudication.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

USSS uses information collected in ALIS to determine whether an applicant is qualified for the relevant vacancy and to track the applicant's progress through the various hiring stages, including the background investigation phase of the hiring process. Aggregated statistics may also be retrieved from the system in conjunction with congressional reporting requirements or in response to other inquiries.

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. ALIS is not used to discover predictive patterns or anomalies. The database contains applicant records that are managed individually.

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

No. There are no other components with assigned roles within the system.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a privacy risk that authorized users could use the 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 ALIS. Further, the most sensitive information in an applicant case file is accessible only to designated personnel in SMD. Additionally, all users undergo training on handling privacy sensitive information each year.

Section 4.0 Notice

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

Individuals are electronically provided notice during the application process on what information is collected and its intended usage as part of the application and background investigation forms they fill out.

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

Applicants enter into the hiring and investigation process voluntarily and may terminate the process at any time for any reason. Declining to provide information simply means that the individual chooses not to participate in the hiring process for that employment opportunity.

Additionally, when filling out the SF-86 form, applicants are given detailed notice that government and private records will be obtained as part of the applicant investigation and hiring process. Applicants are given the opportunity to consent or decline to authorize the release of information about themselves, including medical information if relevant.

At the end of the SF-86, applicants certify, via signature, that statements and attachments within the form are true, complete, and correct to the best of their knowledge and belief and are made in good faith. Applicants certify that they have carefully read the instructions to complete the form and that they understand that a knowing and willful false statement on the form can be punished by fine or imprisonment or both. Lastly, applicants certify that they understand that intentionally withholding, misrepresenting, or falsifying information may have a negative effect on their security clearance, employment prospects, or job status, up to and including denial or revocation of security clearance, or removal and debarment from Federal service.

New hire employees are also given the opportunity to decline to provide their own information by opting to participate in only benefit programs of their choosing. Declining to provide his or her information will prevent the new hire employee from enrolling in that benefit program.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that the applicant lacks sufficient knowledge about the opt-out process.

Mitigation: At each stage of the hiring process, applicants are required to sign release forms authorizing the release of credit, medical, and background investigation information. By signing the releases, the applicants acknowledge that they are advancing to the next stage in the hiring process. Opting out is available at any stage, and USSS investigators are instructed to inform the applicant of the impacts of opting out of a stage in the process.

Section 5.0 Data Retention by the project

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

Dispositions of routine recruitment files such as those contained within the ALIS are governed by the OPM guidance in the Delegated Examining Operations Handbook, Appendix C, Records Retention and Disposition Schedule and the National Archives and Records Administration.

Employee management administrative records will be destroyed when three years old, in accordance with General Records Schedule (GRS) 2.2, item 010. Job vacancy case files will be destroyed when two years old, in accordance with GRS 2.1, items 050 and 051.

For retention and disposition purposes, personnel security and access clearance records of rejected employees are divided into two categories:

- 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 held for 2 years after the corresponding vacancy case file is closed, then destroyed. (See GRS 2.1, Item 50.)
- Records for those applicants 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 5.6, Item 180.)

Applicant tracking data will be destroyed or deleted when three years old, according to GRS 4.1, item 010, and vacancy tracking data will be destroyed or deleted when two years old, according to GRS 4.1, item 010.

Records in ALIS are maintained solely for tracking an applicant throughout the hiring process until he or she is accepted or rejected for USSS employment. ALIS users perform an annual, manual purge of PII based on NARA retention periods. Exceptions to retention schedules may occur when records are retained to support procedural or legal challenges related to the hiring process (e.g., when the USSS is subject to a litigation hold due to a pending legal challenge).

5.2 Privacy Impact Analysis: Related to Retention

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

Mitigation: This risk is partially mitigated through the provision of proper records retention training to all system users and the periodic auditing of the system. ALIS users perform an annual, manual purge of PII based on NARA retention periods. ALIS follows the retention schedule of two years for applicants who are rejected or who withdraw before a Background Investigation, and five years for applicants who are rejected or who withdraw after a Background Investigation.

Privacy Risk: There is a risk that the annual, manual purge of PII will result in information being kept longer than the NARA-approved retention schedules, particularly if a retention schedule does not align with the annual purge schedule.

Mitigation: This risk is currently unmitigated. However, USSS is developing and will be implementing the capability to automatically purge data based on the pre-determined retention periods.

DHS Privacy Office Recommendation: The DHS Privacy Office recommends that USSS implement an automatic purge capability that deletes data once the retention schedule is completed, rather than a purge that occurs at a pre-set interval (e.g., annually) unrelated to specific retention schedules.

Section 6.0 Information Sharing

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

Non-identifying, statistical information concerning USSS hiring may be shared outside DHS. Requests for information in ALIS that contain PII are processed in accordance with the applicable SORN. Records maintained within ALIS may be disclosed to the Department of Justice or another federal agency that is conducting litigation or in proceedings before any court, adjudicative or administrative body, when it is necessary to the litigation. For example, applicants may challenge a determination made by the agency in the course of the hiring process and information in ALIS may be needed in conjunction with such an administrative claim or in litigation.

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

Per the DHS/USSS-003 Non-Criminal Investigation Information System SORN, OPM/GOVT-5 Recruiting, Examining, and Placement Records SORN, and DHS/ALL-023 Personnel Security Management System SORN, routine disclosures of records maintained within ALIS include: to the Department of Justice or other federal agency conducting litigation or in proceedings before any court, adjudicative, or administrative body, when it is necessary to the litigation; and to a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains. For example, as stated above, applicants may challenge investigatory material compiled during a background check made by the agency in the course of the hiring process, or information in ALIS may be needed in conjunction with such an administrative claim or in litigation in regards to a data breach. Additionally, applicants may contact a Member of Congress to inquire as to the status of their application with the USSS, and information in ALIS may be disclosed in order to respond to such an inquiry. These disclosures are either required by Office of Management and Budget policy or necessary to ensure the resolution of legal disputes or questions raised by the applicant.

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.

No information beyond non-identifying statistical information is routinely shared externally. Any Congressional inquiries that may contain PII are tracked via the DHS Executive Secretary (Execsec) Router, although such inquiries are rare.

6.5 Privacy Impact Analysis: Related to Information Sharing

<u>**Privacy Risk**</u>**:** 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 USSS employees in the furtherance of their respective duties. Authorized USSS employees may share information only pursuant to routine uses specified in the above-mentioned SORNs.

Section 7.0 Redress

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

Applicants not selected for employment are notified in writing with a reason for non-selection, such as credit problems, criminal record, or inaccurate information submitted in the application. The DHS Secretary has exempted some records contained in the ALIS system from certain provisions of the Privacy Act, as reflected in DHS/ALL-023 Personnel Security Management 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 Freedom of Information Act (FOIA) Officer, Communications Center (FOIA/PA), 245 Murray Lane, Building T-5, Washington, D. C. 20223, as specified in the DHS/USSS-003 Non-Criminal Investigation Information System SORN, OPM/GOVT-5 Recruiting, Examining, and Placement Records SORN, and DHS/ALL-023 Personnel Security Management System SORN.

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 applicant by the investigator during the interview process. The applicant will have the opportunity to discuss any discrepancies and provide evidence to correct any erroneous information as previous specified within the appeals process discussed in section 2.5.

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

Information collected is provided by the applicant and compared against public, government, or private sources. Any discrepancies identified are communicated to the applicant for clarification and correction during the interview process. The interview process includes both a pre-investigation interview and a post-investigation interview. Both interviews with the applicant are used to ensure the adequacy of the information provided on investigative forms for efficient completion of the investigation which the investigator will subsequently conduct or has completed.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a privacy risk that information stored on applicants is not accurate and thus 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 that information is then cross checked for verification. Information is also confirmed in interviews with applicants, and applicants are given the opportunity to clarify discrepancies. USSS investigators are also aware that some commercial data is not always correct and must be validated.

Applicants have the option to redress any incorrect data via Federal Credit Reporting Act (FCRA) with respect to credit information. Further, redress is available through written request to the Secret Service's FOIA Officer as described above; however, providing an individual access and/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

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 ALIS 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 SMD. 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?

Users granted access to ALIS must receive authorization from designated TAD representatives. Access to the system is limited to those individuals with a direct need to either create records or use the records to make a hiring or clearance determination. Authorized users are then added to predefined functional roles with defined permissions through Active Directory. Authorized personnel access ALIS 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 approved TAD, SMD, and the Application Development Team personnel. Access control into the ALIS application is controlled by the Enterprise Microsoft Active Directory database, which provides ALIS with lookup capabilities to the ePerson system for attribute information such as office location, phone number, and organizational assignment. The ALIS database is provided and maintained by the Application Provisioning System (APS) General Support 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?

Information sharing agreements are reviewed and approved by the program manager, the USSS Privacy Officer, and the USSS Office of Chief Counsel for consistency with applicable laws, regulations, and policies governing the appropriate sharing of PII outside of the Department.

Responsible Officials

Susan Yarwood
Branch Chief, Human Resources
United States Secret Service

Christal Bramson
Acting Privacy Officer
United States Secret Service

Approval Signature

[Original copy signed and on file with the DHS Privacy Office]

____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security