Privacy Impact Assessment
for

Clearances, Logistics, Employees, Applicants, and Recruitment (CLEAR)

DHS/USSS/PIA-013

January 3, 2013

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 (Secret Service or USSS) has created the Clearances, Logistics, Employees, Applicants and Recruitment (CLEAR) Database. CLEAR assists USSS employees in managing applicant data throughout the hiring process. The Secret Service is conducting this Privacy Impact Assessment (PIA) because CLEAR contains personally identifiable information (PII) of persons applying for federal employment with USSS.

Overview

The Security Clearance Division (SCD) manages CLEAR. The system is used to manage and store information related to vacancies and employment applications.

During the application process, SCD personnel receive information from applicants and enter this into CLEAR. As the hiring process proceeds, this information is updated to include results of various assessments, including management interviews, physicals, and polygraphs. Only individuals with a need to know are provided access to CLEAR. This includes specific members of SCD, hiring managers, and polygraph assessors. CLEAR implements a role based access control scheme that provides an appropriate level of access to each individual and prevents excessive data from being revealed.

SCD does not routinely share applicant data with other Departments or components.

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?

Under 5 U.S.C. § 1104, OPM has delegated to agencies the authority to conduct competitive examinations for positions in the competitive service, except for administrative law judge positions. USSS hiring authorities receive their delegation authority from OPM and have two fundamental responsibilities: to ensure that the agency's vacant positions are filled with the best-qualified persons from a sufficient pool of well-qualified eligible candidates; and to uphold the laws, regulations, and policies of merit selection (see 5 U.S.C. §§ 2301 and 2302). Further, the collection of information is authorized by Title 5 of the Code of Federal Regulations, (Administrative Personnel) Sections 100-699.

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

The applicant data in CLEAR is covered by DHS/USSS-003 SORN.

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

CLEAR has received its Authority to Operate, which expires March 2013.

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

Yes. Dispositions of routine recruitment files (such as those contained within the CLEAR system) are governed by the Office of Personnel Management guidance in Delegated Examining Operations Handbook, Appendix C, Records Retention and Disposition Schedule and the National Archives and Records Administration, General Records Schedule 1, Civilian Personnel Records, items 3 and 33b. GRS 23, item 8, also covers the type of "Tracking and Control Files" contained within this system.

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.

During the on-boarding process, new USSS employees must submit the following forms during their orientation sessions to their hiring authority. With the exception of the state tax withholding certificate, which is issued by the appropriate state, all the forms are cleared.

Processing:

- Appointment Affidavit, SF-61
- Employment Eligibility Verification, I-9
- Employee Address, AD-349
- Direct Deposit Sign-Up Form, SF-1199A
- Federal Tax Withholding, W-4
- State Tax Withholding Certificate
- Ethnicity and Race Identification, SF-181
- Self-Identification of Reportable Handicap, SF-256
- Statement of Prior Federal Service, SF-144
- Declaration of Federal Employment, OF-306
- Security Clearance Questionnaire, SF-86

Benefits:

- Designation of Beneficiary (Unpaid Compensation), SF-1152
- Civil Service Retirement System (CSRS) Designation of Beneficiary, SF-2808
- Employee Health Benefits Registration (FEHB), SF-2809
- Life Insurance Election (FEGLI), SF-2817
- Designation of Beneficiary (FEGLI), SF-2823
- Thrift Savings Plan Election, TSP-1
- Thrift Savings Plan Election for Catch-Up Contribution, TSP-1-C
- Designation of Beneficiary (FERS) SF-3102

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.

CLEAR stores information on applicants for federal employment. The information includes:

- First and last name
- Social Security number (SSN)
- Race, gender, and other physically descriptive information
- Employment and all education histories
- Applicant contact information
- Marital status
- Physical results (recorded Pass/Fail)
- 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?

Information is gathered from the applicants themselves in a series of forms, including the SF-86 Questionnaire for National Security Positions. Where required by the nature of the position, additional information may be gathered during interviews, physical exams, and during polygraph assessments. This information is manually entered by authorized users.

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

CLEAR investigators may utilize credit reporting information as well as Lexis/Nexis during the background investigation process.[1] Information collected from the applicant is verified against publicly available, commercially available, or government databases.

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. 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.

[1] For a detailed description of the personnel security process at DHS, please see the DHS/ALL/PIA-038 Integrated Security Management System (ISMS) PIA (March 22, 2011), and the DHS/ALL-023 - Department of Homeland Security Personnel Security Management SORN (February 23, 2010), 75 FR 8088.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Risk: The risk associated with the characterization of the collected information is that inaccurate information could negatively impact an applicant's selection process.

Mitigation: USSS mitigates this risk by collecting information directly from the applicant during the application and clearance process. Only information strictly necessary for completing the clearance process is collected and evaluated.

Information collected from the applicant is verified against publicly available, commercially available, or government databases. Applicant designated references are also interviewed. At the conclusion of this process, the applicant is interviewed and able 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/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.

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 internally to determine the suitability of the applicant to the relevant vacancy. The Agency uses PII directly 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, 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.

Results of internal management assessments are also retained. These 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.

CLEAR 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?

USSS does not routinely share information from CLEAR with any other DHS component or external agency. Prior to being entered in CLEAR, certain minimally necessary applicant information may be shared with other agencies for the purposes of conducting background investigations. For instance, full names and dates of birth are required for criminal background checks, and SSNs are required to locate tax records.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Risk: The privacy risk associated with the uses of the information is that users may employ the information for reasons not consistent with the original purpose.

Mitigation: To mitigate this risk, strict need-to-know and least privilege restrictions are considered when granting access to CLEAR. Further, the most sensitive information in an applicant profile 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. CLEAR collects only information that is strictly necessary for completing the background investigation and applicant hiring missions.

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.

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

Additional notice is provided through the publication of this PIA and DHS/USSS-003 SORN.

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. The applicant may decline to provide specific pieces of information, but this may negatively impact the clearance or employment process.

4.3 Privacy Impact Analysis: Related to Notice

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 releases of credit, medical, and background investigations information. By signing the releases the applicants must acknowledge that they are advancing to the next stage in the hiring process. Opting out is available at any stage and the investigators are instructed to inform the candidate of the impacts of opting out of a stage in the process.

The CLEAR system automatically issues notices to applicants with appropriate redress procedures as well as points of contact embedded within the notice.

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.

Dispositions of routine recruitment files (such as those contained within the CLEAR system) are governed by the Office of Personnel Management guidance in Delegated Examining Operations Handbook, Appendix C, Records Retention and Disposition Schedule and the National Archives and Records Administration, General Records Schedule 1, Civilian Personnel Records, items 3 and 33b. GRS 23, item 8, also covers the type of "Tracking and Control Files" contained within this system. Accordingly, prescribed retention periods are as follows:

a. Applicant tracking data: Destroy/delete when three years old [according to OPM guidance and GRS 1, items 3, & 33b].

b. Vacancy tracking data: Destroy/delete when two years old [GRS 23, item 8].

Records in the CLEAR system 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" orders, etc.).

5.2 Privacy Impact Analysis: Related to Retention

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

Mitigation: Information in CLEAR is maintained in accordance with the approved NARA retention schedule.

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.

Information from CLEAR is not shared outside of DHS.

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

Information from CLEAR is not routinely shared outside of DHS as part of USSS operations.

6.3 Does the project place limitations on re-dissemination?

Information from CLEAR is not routinely shared outside of DHS as part of USSS operations.

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

Information from CLEAR is not routinely shared outside of DHS as part of USSS operations.

6.5 Privacy Impact Analysis: Related to Information Sharing

Information from CLEAR is not shared outside of DHS.

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 CLEAR 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 (FOI/PA), 245 Murray Lane, Building T-5, Washington, D. C. 20223, as specified in the Non-Criminal Investigative Information System SORN.

Contact information and redress procedures are automatically sent out by the CLEAR system after any applicant is not chosen for employment for any reason.

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

Outlined in Section 7.1.

Relevant information uncovered during the background check process is discussed with the applicant by the investigator. The applicant 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?

Outlined above.

7.4 Privacy Impact Analysis: Related to Redress

Risk: There is a 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 their references. This 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 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

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 CLEAR 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 CLEAR 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 that are granted access to the areas of CLEAR that contain individual information must receive authorization from the Chief of the Security Clearance Division, or the Chief's delegated representative. Access to the system will be limited to those individuals with a direct need to either create records or use the records to make a suitability determination.

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 CLEAR and the processes that generate it to be sensitive and for internal use only. It is unlikely that any such agreement or new uses for information would be approved.

Responsible Officials

Keith Hill
Assistant Director – Human Resources and Training

Latita Payne
USSS Privacy Officer

Approval Signature

Original signed and on file with the DHS Privacy Office.

_____

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