Privacy Impact Assessment
for the

Human Resources Business Engine (HRBE)

DHS/CBP/PIA-032

July 25, 2016

Contact Point
Steven Stryk
Office of Human Resources Management (HRM)
Business Process Solutions Division (BPS)
Customs and Border Protection
(202) 863-6184

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

Abstract

Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP) provides Human Resources (HR) services to CBP and other DHS components through a web-based tool called the Human Resources Business Engine (HRBE). HRBE provides case management and HR business process capabilities to CBP and its DHS component customers. The specific HR services vary based on the need and service request of each DHS component customer. CBP is conducting this Privacy Impact Assessment (PIA) because HRBE collects, uses, maintains, and disseminates personally identifiable information (PII) belonging to members of the public and because HRBE provides HR services to multiple DHS components with plans to further expand within the DHS enterprise.

Overview

HRBE, a CBP-owned and developed HR services information technology system, provides case management and business process capabilities for CBP and a limited number of DHS component customers. Although developed originally for CBP, HRBE provides services to other DHS customers, such as: U.S. Immigration and Customs Enforcement (ICE), United States Citizenship and Immigration Services (USCIS), National Protection and Programs Directorate (NPPD), and DHS Headquarters. DHS customers may choose from HRBE's offered HR services to meet their individual HR case management and workflow needs. As other DHS customers request HRBE services, the system has the potential to become an enterprise-wide HR case management system for DHS.

HRBE currently is composed of seventeen distinct HR functions. A list of HRBE functions used by other DHS customers is included in Appendix A, and a list of access levels within each function of the seventeen functions is provided in Appendix B. The seventeen functions are as follows:

1. **Performance Management Function** automates the administration, processing, tracking, and reporting of CBP employees' annual performance plans, covering the initial establishment of each employee's plan, the mid-year review, and the end of year review.
2. **Entry and Professional Level Hiring Function** tracks and manages applicants from the submission of application to actual Entrance on Duty (EOD). Interactions include: text messages from HR staff to applicants to keep them apprised of their application status; access to a tracking application[1] for those applicants who have received a tentative offer for select positions to monitor their hiring status; data exchange of staffing and certificate data between the Office of Personnel Management (OPM) and CBP; data exchange of background investigation information between HR and CBP Office of Professional Responsibility (OPR);

[1] Select applicants are granted access to the Central Application Self-Service (CASS) application. This application provides job application process status for CBP conditional employees, who have passed the entrance exam and been issued a Tentative Selection Letter for an entry-level position in one of these occupations: Agricultural Specialist, Border Patrol Agent, or Border Patrol Officer. CASS provides a status on the following requirements: pre-employment forms, medical exam fitness test, drug screening, structured interview, background investigation, qualifications, and scheduled report date. Login into CASS requires last four digits of social security number and date of birth. CASS is described in the Appendix to the DHS/ALL/PIA-043 Hiring and On-Boarding Process PIA, *available at:* https://www.dhs.gov/sites/default/files/publications/pia-app-update-043-dhs-wide-hiring-and-on-boarding-06252015.pdf.

and scheduling and results of pre-employment tests such as: drug test results (pass/fail only), medical results if required for position suitability, and background investigation results (including polygraph) to obtain required clearances. The actual required pre-employment tests will vary depending on the position for which the applicant is being considered. The Entry and Professional Level Hiring Function does not store the details of an applicant's suitability or pre-employment tests, but rather which tests are required and if they have been passed.

3. **Senior Executive Service (SES) Function**, similar to the preceding function, this function tracks and manages recruitment actions but focuses on senior executive recruitments.
4. **Table of Organization Function** provides the reporting capability to accurately project and compare CBP's federally-funded positions to the CBP mission within budgetary constraints.
5. **Safety Inspection Function** tracks and manages the: scheduling, work flow, processing, results, corrective actions taken, and reporting of safety inspections conducted in the work place. The goals of these inspections are: 1) to ensure safety concerns of those who work in CBP workplaces are addressed and 2) to proactively ensure that CBP workplaces remain compliant with Department of Labor (DOL) Occupational Safety and Health Administration (OHSA) safety standards.
6. **Employee Relations Case Tracking Function** tracks and manages records related to DHS employees' disciplinary, performance, medical, and informal counseling cases. Case status updates and basic personnel information is exchanged with the CBP OPR's Joint Intake Case Management System (JICMS)[2] through a system-to-system data exchange. Labor and Employee Relations staff also are granted limited access to JICMS on a case-by-case basis when they have an official need to know. Investigatory material is not stored in HRBE.
7. **Fitness Function** provides entry of, and access to, fitness exam results administered during the hiring of applicants or (re)certification of employees as determined by the specific position requirements, such as law enforcement positions. This function differs from pre-employment medical tests, which verifies the applicant against medical standards for entry-level law enforcement positions.
8. **Labor Relations Case Tracking Function** tracks and manages labor relations cases such as Unfair Labor Practice claims, grievances, and arbitrations. This function serves as an information resource for the historical activity/status reports and trends for client managers and executive leadership.
9. **Drug Free Workplace Function** maintains records mandated by the Federal Government's comprehensive drug-free workplace program for all Federal Executive Branch workers.[3] It

[2] JICMS is the OPR system used to record misconduct, to conduct criminal and administrative investigations, and to track disciplinary actions related to CBP and U.S. Immigration and Customs Enforcement (ICE) employees and contractors. A PIA is currently being written for JICMS.
[3] Executive Order 12564 - Drug-Free Federal Workplace, 1986, *available at:* http://www.archives.gov/federal-register/codification/executive-order/12564.html.

requires random selection of employees for drug testing and the maintenance of historical drug test results.

10. **Financial Disclosure OGE-450 Function** tracks and manages the data entry, routing, processing, and tracking of financial disclosure forms completed by covered employees annually.

11. **Customer Inquiry Tracking Function** tracks and manages inquiries from employees and applicants via phone, email, or direct contact on various topics/subtopics related to the status of their pending applications or personnel actions.

12. **Retirement Tracking Function** tracks the retirement application from receipt in the HR office to OPM. This function also provides reports to monitor workload and provide metrics.

13. **Background Investigations (BI) Function** initiates with BI process with applicants by forwarding them the link to complete the OPM eQIP[4] form. HR specialists with access to the BI function review the submitted eQIP for completeness, and then forward the eQIP package to the OPR Cornerstone System[5] to initiate the BI process for applicants and employees. It also receives information from OPR when the BI is completed. In addition, this function exchanges information with the DHS Integrated Security Management System (ISMS)[6] nightly to update case information in both systems. The BI Function maintains status and basic biographic information only. HR specialists view the eQIP to verify completeness but do not make any adjudicative decisions. It is a pass-through for the eQIP but does not ingest or retain any information from the eQIP. The BI Function does not maintain investigatory material. The purpose of this module is to manage the case load on HR for eQIP initiations and wait for results from OPR. For a full description of the BI process at CBP, please see the Cornerstone System PIA.

14. **Personnel Action Request Function** allows requesting and approving officials to submit a Request for Personnel Actions to HR for processing; HR specialists to route and code the personnel action; and transmission of data to the United States Department of Agriculture (USDA) National Finance Center (NFC).

15. **Medical and Contracting Officer's Representative (COR) Function** tracks and manages the medical activities associated with an applicant (i.e., scheduling the medical appointment, getting the test results of the medical examination) during the hiring process for the hiring centers. This function also tracks and processes the invoices received for the medical services provided to the applicant during the pre-employment process.

---

[4] eQIP is a secure website managed by OPM that is designed to automate the common security questionnaires used to process federal background investigations. For additional information, please see http://www.opm.gov/privacy/PIAs/eQIP.pdf.

[5] The Cornerstone System facilitates the BI process and improves its efficiency. Cornerstone retrieves information from other systems, compiles the information, and sends the document to the appropriate system for processing. A Cornerstone PIA is forthcoming.

[6] DHS/ALL/PIA-038 Integrated Security Management System (ISMS) (March 22, 2011), *available at: https://www.dhs.gov/sites/default/files/publications/privacy_pia_dhswide_isms-2011.pdf.*

16. **Employee Position Profile Function** supports the look up of positions and employees assigned to the positions in CBP. It also allows HRM and the Program offices to support the tracking of Person or Position data elements that are not supported by NFC (i.e., special initiatives like Trade Revenue and Cybersecurity-designated positions, emergency essential personnel).
17. **Ticketing Function** allows all HRBE users to submit a request to correct a technical error. This module differs from the Customer Inquiry Tracking module, which tracks the incoming requests from employees and applicants regarding the status of the hiring or personnel actions. The Ticketing function is the bug/defect tracking system for HRBE administrators to report issues or request enhancements to the HRBE system.

HRBE Information Sources:

1. Individual Employees (CBP and other DHS component customers)

HRBE is not an employee self-service portal. However, individual employees are able to upload limited information into HRBE for two modules listed above. Individual employees may access HRBE directly for two limited purposes: (1) to review and acknowledge performance management plans and evaluations, and (2) submit required financial disclosure forms. Supervisors and Managers have more roles in HRBE. Supervisors and Managers may use HRBE to: (1) track and measure employee performance, (2) review and select applicants from the available applicant list as part of a hiring action, and (3) generate other personnel requests as needed.

2. HR Users in Performance of Their Official Duties

HR professionals access HRBE directly to provide, obtain, or change information regarding: personnel actions; applicants and hiring activities; medical tests; fitness tests; drug tests; background investigation results; financial disclosures; disciplinary cases; performance cases; safety inspections; customer complaints; labor relations issues; workers compensation cases; and general position information.

Each HRBE Function has its own set of roles with activities and rights unique to that Function (see Appendix B). While HRBE has a single, unified database containing data for all Functions, the data is "partitioned" by the Function and further by component user (CBP, ICE, etc.).

3. Automated Systems/Entities

HRBE also obtains information directly from system-to-system connections or as data extracts from external systems. HRBE obtains contact information for employees and contractors (who require access to HRBE as part of their HR support job duties); applicant and vacancy announcement certificate information; pre-employment scheduling and test results information (i.e., drug, medical, and fitness); job eligibility and ranking for selection; suitability determinations such as the results of background investigation and clearance information; and disciplinary, performance, medical, and counseling information. Descriptions of the types of information obtained from these system sources and how HRBE interacts with these systems are provided in Section 2.2.

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?

HRBE is authorized to collect general personnel record, employee performance files, safety inspection, and medical file data under the following authorities defined in 5 U.S.C. §§ 301, 1104, 1302, 1303, 2302(b)(10), 2951, 3109, 3301, 3302, 3304, 3305, 3306, 3307, 3309, 3313, 3317, 3318, 3319, 3321, 3326, 3372, 4103, 4118, 4305, 5112, 5405, 5532, 5533, 8145, and 8347. Executive Orders 9397 as amended by 13478, 9830, 10450, and 12107 authorize the use and dissemination of PII including Social Security numbers (SSN) for the uniform and orderly administration of personnel records.

DHS has established a Service Level Agreement (SLA) with the United States Department of Agriculture's (USDA) National Finance Center (NFC) that provides authority for DHS components, including CBP, to use both human capital and payroll/personnel information technology systems to perform agency administration functions.

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

To permit the collection of various types of records for numerous HR and personnel actions, HRBE relies on the following SORNs:

For formal personnel actions and records, relating to all aspects of federal employment:

- OPM/GOVT-1 General Personnel Records[7] SORN provides overall coverage for factual information maintained about a person's federal employment while employed and after separation. Records in this system have various uses by agency personnel offices, including screening qualifications of employees; determining status, eligibility, and employee's rights and benefits under pertinent laws and regulations governing federal employment; computing length of service; and other information needed to provide personnel services. These records may also be used to locate individuals for personnel research. This SORN provides overall coverage for the following HRBE functions: Entry and Professional Level Hiring; Retirement Tracking; Personnel Action Request; and Medical and COR.
- OPM/GOVT-2 Employee Performance File System Records[8] SORN provides coverage for records maintained to ensure that all appropriate records on an employee's performance are retained and are available: (1) To agency officials having a need for the information; (2) to employee's; (3) to support actions based on the records; (4) for use by the OPM in connection with its personnel

[7] OPM/GOVT-1 General Personnel Records (December 11, 2012), 77 FR 73694, *available at:* https://www.gpo.gov/fdsys/pkg/FR-2012-12-11/html/2012-29777.htm.
[8] OPM/GOVT-2 Employee Performance File System Records (June 19, 2006), 71 FR 35342, *available at:* https://www.gpo.gov/fdsys/pkg/FR-2006-06-19/html/06-5459.htm.

management evaluation role in the Executive Branch; and (5) to identify individuals for personnel research. This SORN provides coverage for the Performance Management function in HRBE.

- OPM/GOVT-3 Records of Adverse Actions, Performance Based Reduction in Grade and Removal Actions, and Termination of Probationers[9] SORN provides coverage for records resulting from the proposal, processing, and documentation of adverse actions taken either by OPM or by agencies against employees. This SORN covers the Employee Relations Case Tracking function in HRBE.

- OPM/GOVT-5 Recruiting, Examining, and Placement Records[10] SORN provides coverage for records used in considering individuals who have applied for positions in the federal service by: making determinations of qualifications including medical qualifications, for positions applied for, and to rate and rank applicants applying for the same or similar positions. They are also used to refer candidates to federal agencies for employment consideration, including appointment, transfer, reinstatement, reassignment, or promotion. Records derived from OPM or agency assessments used to determine training needs of participants. These records may also be used to locate individuals for personnel research. This SORN provides additional coverage for Entry and Professional Level Hiring, Entry and Professional Level Hiring, and Personnel Action Request functions.

- OPM/GOVT-6 Personnel Research and Test Validation Records[11] SORN provides coverage for records collected, maintained, and used by OPM or other federal agencies for the construction, analysis, and validation of written tests and other assessment instruments used in personnel selection and appraisal, other assessment instruments used in personnel selection and appraisal, and for research on and evaluation of personnel/organizational management and staffing methods, including workforce effectiveness studies. This SORN provides general coverage for the sharing of information maintained within HRBE for general research purposes.

- OPM/GOVT-7 Applicant Race, Sex, National Origin and Disability Status Records[12] SORN provides coverage for records used by OPM and agencies to: 1) Evaluate personnel/organizational measurement and selection methods; 2) Implement and evaluate agency affirmative employment programs; 3) Implement and evaluate agency Federal Equal Opportunity; 4) Recruitment Programs (including establishment of minority recruitment files); 5) Enable OPM to meet its responsibility to assess an agency's implementation of the Federal Equal Opportunity Recruitment Program; 6) Determine adverse impact in the selection process as required by the Uniform Guidelines cited in the Authority section above; 7) Enable reports to be prepared regarding breakdowns by race, sex, and national origin of applicants (by exams taken, and on the selection of such applicants for

[9] OPM/GOVT-3 Records of Adverse Actions, Performance Based Reduction in Grade and Removal Actions, and Termination of Probationers (April 27, 2000), 65 FR 24732, *available a*t: https://www.gpo.gov/fdsys/pkg/FR-2000-04-27/html/00-10088.htm.
[10] OPM/GOVT-5 Recruiting, Examining, and Placement Records (June 19, 2006), 71 FR 35351, *available at:* https://www.gpo.gov/fdsys/pkg/FR-2014-03-26/html/2014-06593.htm.
[11] OPM/GOVT-6 Personnel Research and Test Validation Records (June 19, 2006), 71 FR 35354, *available at:* https://www.gpo.gov/fdsys/pkg/FR-2006-06-19/html/06-5459.htm.
[12] OPM/GOVT-7 Applicant Race, Sex, National Origin and Disability Status Records (June 19, 2006), 71 FR 35356, *available at:* https://www.gpo.gov/fdsys/pkg/FR-2006-06-19/html/06-5459.htm.

employment); and 8) To locate individuals for personnel research. This SORN provides coverage for the Table of Organization and Employee Position Profile functions in HRBE.

For collection of Contractor Information (who require access to HRBE as part of their HR support job duties):

- DHS/ALL-021 Department of Homeland Security Contractors and Consultants SORN[13] provides coverage for records used by DHS to collect and maintain records on DHS contractors and consultants.

For Employee Relations, Internal Affairs, and Professional Responsibility records and background investigations:

- DHS/ALL-018 Department of Homeland Security Grievances, Appeals, and Disciplinary Action Records System of Records[14] SORN provides coverage for records used to document all current and former DHS personnel who have been the subject of proposed or final disciplinary action, have filed a grievance or appeal, or have been suspected of misconduct. This SORN provides coverage for Employee Relations Case Tracking function.

Note that internal affairs records and personnel security records are not stored in HRBE and therefore no SORN coverage is required. These records are stored in JICMS and Cornerstone, respectively.

For Labor Relations cases and related records:

- OPM/GOVT-9 File on Position Classification Appeals, Job Grading Appeals, Retained Grade or Pay Appeals, Fair Labor Standard Act (FLSA) Claims and Complaints, Federal Civilian Employee Compensation and Leave Claims, and Settlement of Accounts for Deceased Civilian Officers and Employees File on Position Classification Appeals, Job Grading Appeals, and Retained Grade or Pay Appeals, and Fair Labor Standard Act (FLSA) Claims and Complaints[15] SORN provides coverage for records primarily used to document the processing and adjudication of a position classification appeal, a job grading appeal, a retained grade or pay appeal, FLSA claim or complaint, compensation and leave claims, or disputes concerning the settlement of the account for a deceased federal civilian officer or employee. This SORN provides coverage for the Labor

[13] DHS/ALL-021 Department of Homeland Security Contractors and Consultants System of Records (October 23, 2008), 73 FR 63179, *available at: https://www.gpo.gov/fdsys/pkg/FR-2008-10-23/html/E8-25205.htm*.
[14] DHS/ALL-018 Department of Homeland Security Grievances, Appeals, and Disciplinary Action Records System of Records (October 17, 2008), 73 FR 61882, *available at:* https://www.gpo.gov/fdsys/pkg/FR-2008-10-17/html/E8-24741.htm.
[15] OPM/GOVT-9 File on Position Classification Appeals, Job Grading Appeals, Retained Grade or Pay Appeals, Fair Labor Standard Act (FLSA) Claims and Complaints, Federal Civilian Employee Compensation and Leave Claims, and Settlement of Accounts for Deceased Civilian Officers and Employees File on Position Classification Appeals, Job Grading Appeals, and Retained Grade or Pay Appeals, and Fair Labor Standard Act (FLSA) Claims and Complaints (October 1, 2013), 78 FR 60331, available at:https://www.gpo.gov/fdsys/pkg/FR-2013-10-01/html/2013-23839.htmhttps:/www.gpo.gov/fdsys/pkg/FR-2013-10-01/html/2013-23839.htm.

Relations Case Tracking function and in certain circumstances the Customer Inquiry Tracking function.

- EEOC/GOVT-1 Equal Employment Opportunity in the Federal Government Complaint and Appeal Records[16] SORN provides coverage for records maintained for the purpose of enforcing the prohibitions against employment discrimination contained in the Age Discrimination in Employment Act, the Equal Pay Act and section 321 of the Government Employees Rights Act of 1991. This SORN provides coverage for the following HRBE functions: Labor Relations Case Tracking and Customer Inquiry Tracking.

- DOL/GOVT-1 Office of Worker's Compensation Programs (OWCP), Federal Employees' Compensation Act File[17] SORN provides coverage for processing and adjudicating claims that federal employees and other covered individuals file with the Department of Labor's OWCP seeking monetary, medical, and similar benefits for injuries or deaths sustained while in the performance of duty. The records provide information and verification about the individual's employment-related injury and the resulting disabilities and/or impairments, if any, on which decisions awarding or denying benefits provided under the Federal Employees' Compensation Act (FECA) must be based. This SORN provides coverage for the Safety Inspection and Labor Relations Case Tracking HRBE functions.

For medical information, fitness tests, and drug testing information:

- OPM/GOVT-10 Employee Medical File System Records[18] SORN provides coverage for the collection of medical records for a wide range of purposes, such as: 1) To comply with existing DOL OSHA and OWCP regulations; 2) To provide an accurate medical history of the total health care, as well as occupation or hazard exposure documentation, and health monitoring in relation to health status and claims of the individual; 3) To provide a legal document describing the health care administered and any exposure incident; 4) To ensure that all relevant, necessary, accurate, and timely data are available to support any medically-related employment decisions affecting the subject of the records (e.g., in connection with fitness-for-duty and disability retirement decisions); 5) To document claims filed with and the decisions reached by OWCP and the individual's possible reemployment rights under statutes governing that program; 6) To document employee's reporting of on-the-job injuries or unhealthy or unsafe working conditions, including the reporting of such conditions to OSHA and actions taken by that agency or by the employing agency; 7) To ensure proper and accurate operation of the agency's employee drug testing program under Executive Order 12564. This SORN provides coverage for the following HRBE functions: Fitness, Drug Testing, Safety Inspections, and Entry and Professional Level Hiring.

[16] EEOC/GOVT-1 Equal Employment Opportunity in the Federal Government Complaint and Appeal Records (July 30, 2002), 67 FR 49338, *available at:* https://www.gpo.gov/fdsys/pkg/FR-2002-07-30/html/02-18895.htm.
[17] DOL/GOVT-1 Office of Worker's Compensation Programs, Federal Employees' Compensation Act File (January 11, 2012), 77 FR 1738, *available at:* https://www.gpo.gov/fdsys/pkg/FR-2012-01-11/html/2012-345.htm.
[18] OPM/GOVT-10 Employee Medical File System Records (June 21, 2010), FR 73694, *available at:* https://www.gpo.gov/fdsys/pkg/FR-2010-06-21/html/2010-14838.htm.

- DHS/ALL-022 Department of Homeland Security Drug Free Workplace[19] SORN provides coverage for records to maintain information gathered by and in the possession of DHS Drug Free Workplace Program Officials, used in the course of their duties to verify positive test results for illegal use of controlled substances, as well as collect and maintain evidence of possession, distribution, or trafficking of controlled substances. This SORN provides coverage for the Drug Free Workplace, and Background Investigations HRBE functions.

- DHS/ALL-004 General Information Technology Access Account Records System (GITAARS)[20] SORN provides coverage for records collected to provide authorized individuals access to, or interact with DHS information technology resources and allow sharing of information between individuals in the same operational program to facilitate collaboration. This SORN provides coverage for HRBE users to gain access to and share information with those within DHS who have an official need to know.

For customer inquiries, comments, and complaints:

- DHS/ALL-016 Department of Homeland Correspondence Records System[21] SORN provides coverage for managing incoming information and responses to inquiries, comments, or complaints made to DHS. This SORN provides coverage for Customer Inquiry Tracking function used by both DHS Headquarters and CBP.

For ethics programs and financial disclosure forms:

- OGE/GOVT-1 Executive Branch Personnel Public Financial Disclosure Reports and Other Name-Retrieved Ethics Program[22] SORN provides coverage for the all records maintained in accordance with the requirements of the Ethics in Government Act of 1978 and the Ethics Reform Act of 1989. These records include the filing of required financial records, reports concerning certain agreements between the covered individual and any prior private sector employer, ethics agreements, and the preservation of waivers issued to an officer or employee pursuant the Ethics Reform Act. This SORN provides coverage for the Financial Disclosure OGE-450 HRBE function.

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

Yes, the most recent security plan for HBRE was completed on September 1, 2015. HRBE will be issued a valid Authority to Operate, pending the publication of this PIA.

---

[19] DHS/ALL-022 Department of Homeland Security Drug Free Workplace (October 31, 2008), 73 FR 64974, *available at:* https://www.gpo.gov/fdsys/pkg/FR-2008-10-31/html/E8-25971.htm.
[20] DHS/ALL-004 General Information Technology Access Account Records System (GITAARS) (November 27, 2012), 77 FR 70792, *available at:* https://www.gpo.gov/fdsys/pkg/FR-2012-11-27/html/2012-28675.htm.
[21] DHS/ALL-028 Department of Homeland Security Correspondence Records System (November 10, 2008), 73 FR 66657, *available at:* https://www.gpo.gov/fdsys/pkg/FR-2008-11-10/html/E8-26691.htm.
[22] OGE/GOVT-1 Executive Branch Personnel Public Financial Disclosure Reports and Other Name-Retrieved Ethics Program (May 8, 2003), FR 24744, *available at: https://www.gpo.gov/fdsys/pkg/FR-2003-01-22/html/03-1101.htm*.

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

Yes, NARA has approved Government-wide record schedules for HR-related functions. Most of these schedules can be found in NARA's General Record Schedules 1 and 2. General Records Schedule 2.8: Employee Ethics Records, provides disposition authority for records Executive Branch agencies to create and receive in the course of carrying out their ethics program responsibilities, including OGE Form 450 Confidential Financial Disclosure Reports.[23] A comprehensive list of retention schedules by general HR category and SORN coverage can be found in Appendix C.

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.

The vast majority of HR forms used to collect information from members of the public originate with the agencies responsible for the Government-wide governance of these functions. As a result, the PRA obligation resides with these agencies. Such agencies include: OPM, Department of Labor (DOL), Department of Health and Human Services (HHS), Equal Employment Opportunity Commission (EEOC), Merit Systems Protection Board (MSPB), and Office of Government Ethics (OGE).

Section 2.0 Characterization of the Information

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

HRBE collects, uses, and maintains information about applicants for employment, current employees, and contractors who require access to HRBE as part of their HR support job duties.

For Applicants:

HRBE collects and maintains the following information on applicants: position title, series, grade, total number of applications, number of eligible applicants, number of ineligible applicants, certificate name, certificate issue date, certificate due date, names of applicants referred, names of applicants selected, names of applicants that declined, SSN, date the certificate must be returned, certificate audit date, written examination results, current status in the employment process, fitness results, oral examination results, background investigation pass/fail results, language results, medical results, drug test results, and contact information (telephone numbers, emergency contact).

For Employees:

[23] http://www.archives.gov/records-mgmt/grs/grs02-8.pdf.

In addition to the applicant information mentioned above, once the applicant becomes an employee, HRBE collects and maintains the following information on employees: name, SSN, home and work addresses, email address, work and home phone numbers, race and national origin, duty station, service dates, date of birth, work schedule, retirement eligibility, organization, gender, entrance on duty date, veterans preference code, supervisory code, type of appointment, pay plan, retirement type, salary, disability, sex code, education data, additional data to establish an employee's personnel record, and case data (certain functions provide specific information (i.e., Employee Relations, Labor Relations, Safety Inspections, Performance, Financial Disclosure, Retirement, Personnel Action, Ticketing, and Customer Inquiry case information)).

For Contractors:

HRBE collects and maintains the following information about contractors who require access to HRBE as part of their HR support job duties: name, SSN, work and home addressees, contractor indicator, office information, home and work phone numbers, and email addresses.[24] HRBE does not collect information about all contractors within CBP or other DHS customer components. HRBE is not used for contractor management or personnel actions.

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

HRBE information is collected from two primary sources: individuals and other systems.

Individuals:

Applicants:

Information is obtained from the applicant primarily through OPM hiring systems. Applicants provide their basic contact information and supporting documents, such as: resumes, answers to position-specific questions, veteran's preference, etc., through the USAJOBS[25] website, which is entered into OPM's Application Manager.[26] Application Manager is used to determine if the applicant's qualifications meet the minimum qualification requirements for the vacancies for which they have applied. Applicant information uploaded into Application Manager is made available to HR specialists via secure login to the OPM USA Staffing[27] to rank and rate eligible candidates for the position.

Employees:

Federal employees, in a variety of roles as a manager, a supervisor, an employee, an HR staff member, and/or a financial disclosure filer, enter information directly into HRBE. HRBE collects

[24] Contractor information is obtained from CBP WebTELE system, described in section 2.2.
[25] 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, please see http://www.opm.gov/privacy/PIAs/USAJOBS.pdf.
[26] Application Manager is a standalone, browser-based online tool owned and managed by OPM that is used exclusively by applicants to apply for federal jobs.
[27] USA Staffing is used to collect information from applicants for federal jobs to determine if their qualifications meet qualifications requirements for the vacancies for which they have applied.

performance-related information from a manager, supervisor, and employee throughout the year. HR staff also enters information directly into HRBE to record activities and documents associated with a particular case.

Contractors:

Contractors (who require access to HRBE as part of their HR support job duties) provide initial and periodic updated information about themselves through the CBP WebTELE application housed on the CBP intranet. The information provided includes: name, general business contact information, organizational domain, login name, and email address.

Information from Other Systems:

HRBE interacts with many different systems in a variety of ways to send and receive information.

- USDA National Finance Center (NFC) Personnel/Payroll System (PPS): HRBE receives employee demographic and position information from the USDA NFC PPS via a bi-weekly data feed using File Transfer Protocol (FTP) for case management and personnel action processing purposes. HRBE also sends employee and position information to the USDA NFC PPS using the same FTP on a daily basis to establish, maintain, and retire personnel records.
- DHS Integrated Security Management System (ISMS) Enterprise Data Warehouse (EDW): HRBE sends and receives personnel security information from the ISMS EDW via a web service (machine-to-machine communication over the World Wide Web) using Secure Socket Layer (SSL) and Transport Layer Security (TLS) protocols. ISMS provides HRBE with the suitability status of applicants and employees for existing cases, and HRBE provides ISMS with new or changed personnel information.
- USA Staffing: OPM's USA Staffing system provides HRBE with information using secure FTP for file transfers. USA Staffing provides three different types of information: vacancy announcement, position, and certificate. Upon receipt of the certificate, hiring officials may enter USA Staffing directly to obtain additional selection information such as resumes and responses to questions posted in the announcement, but these actions are taken outside of HRBE.
- Comprehensive Health Services (CHS): CBP contracts with CHS to provide services for scheduling pre-employment health tests and providing results to CBP. HRBE sends and receives applicant information, pre-employment scheduling requests, and test results information via web services over TLS or HyperText Transfer Protocol (HTTP) over Secure Socket Layer (SSL). The information is used to schedule applicants for pre-employment tests (drug, medical, fitness) and to determine job eligibility and ranking for job selection.
- DHS Email as a Service: HRBE obtains email addresses for employees and contractors from the DHS email system. This information is used to send email notifications and reminders to affected parties regarding actions taken (e.g., a promotion action was

processed effective on this date) or actions to be taken (e.g., approve an employee's performance plan).

- Directory System (WebTELE): HRBE receives general contact and biographic information about CBP employees and CBP contractors (who require access to HRBE as part of their HR support job duties) directly from the CBP Directory System, known as WebTELE, to verify the individual is currently employed by (or under contract with) CBP, and therefore can access HRBE. The biographic information provided by WebTELE includes the following information: name, organizational domain, login name and email address.
- Client User Loads: Each DHS Component that uses HRBE identifies who will use HRBE for a particular function and provides CBP with minimal Active Directory information in order to establish an account in HRBE for user access for customers outside CBP.
- Joint Intake Case Management System[28] (JICMS): HRBE sends and receives disciplinary, performance, medical, and counseling information about DHS-related cases referred to the Joint Intake Center via a web service (machine-to-machine communication over the World Wide web) using Secure Socket Layer (SSL) and Transport Layer Security (TLS) protocols. The specific information provided by JICMS, as the source system, to HRBE includes: SSN, case number, type of allegation, incident date, and name of JICMS team assigned to the case. This information is only used by HR staff in performance of the Employee Relations Case Tracking Function.
- Employees' Compensation Operations & Management Portal (ECOMP): HRBE receives information on federal employees injured at work that have filed a claim under the Federal Employees' Compensation Act via secure HTTP over SSL from a vendor with which CBP has a contract.

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

No. HRBE does not use information from commercial sources or directly from publicly available data. OPR may collect information during the background investigation process, but investigatory material is not stored in HRBE.

2.4 Discuss how accuracy of the data is ensured.

Applicant and new employee information is collected directly from the individual. Because the individual provides the majority of information about him or herself directly, the likelihood of erroneous PII is minimized. Identity is verified through the examination of documents such as passport, driver's license, birth certificate, and Social Security card, and third-party concurrence such as references. Any

[28] JICMS does not currently have a PIA on file with the DHS Privacy Office. The JICMS PIA is forthcoming.

further actions taken or based on submitted information must be properly vetted and researched through appropriate channels (such as the Personnel Security Office).

Human Resource Specialists, Administrative Officers, supervisors, managers, and other individuals authorized to review data accuracy perform quality control checks before information is entered into HRBE from HR forms. These individuals will notify the affected individual when there appears to be an inaccuracy and request that the individual correct the data before it is entered into the system.

Employees can check their personnel and payroll data by viewing the Statement of Earnings and Leave (SEL), W-2 Forms, or information screens available through the employee self-service system provided by the Agency.

Employees may use the web-based OPM Electronic Official Personnel Folder (eOPF) system to view and check official documents, Notification of Personnel Action forms, and associated supporting documents. For security purposes, an individual PIN number may be required to view this information.

Information received from a court or tax authority is assumed to be accurate.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk of over collection of information because HRBE may store BI information, as well as sensitive internal affairs investigatory information maintained in JICMS.

Mitigation: This risk is mitigated by limiting the information stored in HRBE to the information needed to perform HR functions. BI information in HRBE is limited only to the pass or fail decision made about selected applicants. This BI information is needed to support of the hiring process.

JICMS, the CBP internal affairs system, shares select information with the Employee Relations Case Tracking Function in HRBE in order for HRBE to create a case to support disciplinary and personnel actions. The information provided by JICMS consists of the following data fields: SSN, case number, type of allegation, incident date and the name of the JICMS team assigned to a particular case. Once the case is created in HRBE, HRBE sends the case information back to JICMS to facilitate case tracking between the HRBE Employee Relations Case Tracking Function and JICMS. HRBE access to this information is limited to those who: 1) have access to the Employee Relations Case Tracking Function and 2) who are assigned to that particular case and therefore have an official need to know.

Privacy Risk: HRBE maintains information about individuals that are not selected for federal employment.

Mitigation: This risk is mitigated by limiting the information stored in HRBE to the information needed to perform HR functions. HRBE does not collect nor maintain information about individuals who were not selected for federal employment. Since HRBE maintains records needed during the pre-employment and hiring process, HRBE only maintains information about applicants who were selected for DHS positions.

In the event that the selected applicant elects not to accept the position or fails to meet the hiring criteria, the information is maintained for three years. This practice allows HRBE to efficiently leverage

existing applicant information against multiple applications submitted by the same applicant within the three-year period.

Privacy Risk: There is a risk of over collection, because HRBE maintains copies of records that are also maintained by OPM and USDA/NFC.

Mitigation: HRBE does not duplicate official records maintained in other systems. For example, HRBE does not maintain the Standard Form 50 (SF-50) Notice of Personnel Action because this form is maintained in the OPM-owned electronic Official Personnel File (eOFP). However, HRBE does maintain the SF-52 Request for Personnel Action because this form provides a worksheet for use by agencies to request official personnel actions. HRBE maintains this form because OPM does not maintain the agency's history of requests nor the approvals associated with these requests.

Privacy Risk: HRBE may collect more information than is necessary and relevant to accomplish HRBE's HR functions.

Mitigation: HRBE performs a broad scope of HR functions, thus collecting a large amount of information. The type of information collected from a user or about an individual will vary with the need for the information and the function for which it is collected. Staff are trained in what information is necessary and relevant for each specific function. For example, the information collected about an applicant will differ from the information collected to resolve a disciplinary case or document employee performance.

To maintain the confidentiality of certain functions, such as disciplinary or performance information and limit access to those with an official need to know, HRBE segregates data by Function, component, organization, and individual user roles. This separation limits user access to information necessary and relevant to a particular user with an official need to know. HRBE only uses and displays SSN to de-conflict between applicants or employees with identical names. This is critical when ordering tests such as a medical examination, drug test, or background investigation, or to request a personnel action.

Privacy Risk: For information collected from other systems, there is a privacy risk that information about individuals may be inaccurate.

Mitigation: To increase the accuracy of the information, information is collected directly from the individual when possible. Examples of direct collections include information collected from individuals during the hiring and on-boarding process, as well as the submission of forms, such as financial disclosure forms, worker's compensation forms, and grievance forms. Collecting information from the individual increases the likelihood that the information is accurate. Additionally, individuals may monitor information about themselves, such as performance plans and evaluations through the performance management function, and personnel actions through the Electronic Official Personnel File (eOPF)[29] website.

While HRBE is not a self-service portal, employees can check their personnel and payroll data by viewing the Statement of Earnings and Leave (SEL), W-2 Forms, or information screens available through other employee self-service systems provided by CBP or DHS component customers. If self-service options are unavailable or unsuccessful, individuals may also a Privacy Act request for correction or amendment.

[29] https://eopf.nbc.gov/opm/.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

CBP and DHS component customers use HRBE to accomplish various HR functions, such as: make qualification and hiring selection decisions; plan and evaluate employee performance; initiate and track personnel action requests; accept and maintain employee financial disclosure reports; maintain pass or fail results for: background investigation, drug testing, and fitness exam; maintain reports for safety inspection results; track disciplinary, performance, medical, and informal counseling cases; provide the Table of Organization tool to monitor federal positions against budget limits; track unfair labor practice claims, grievances, and arbitrations; track retirement applications; and submit requests to correct technical errors or enhancements in HRBE.

HRBE uses the SSN as the primary unique identifier for all HR records in HRBE. It allows HRBE to correlate information from a variety of HR sources and associate the information with the individual. HRBE displays a truncated SSN on case screens to mask the entire SSN. Only individuals with an official "need-to-know" related to their job function may access SSNs.

HRBE also uses information to record, process, track, and report on the status of HR cases. HRBE creates case management information to support various lines of business requirements for CBP and DHS component HRBE users. Standard reports are available in every HRBE workflow based on user requirements. There is also a simple ad-hoc query function available to easily retrieve workflow data based on selection criteria specific to the case. HRBE users may run reports to meet internal and external reporting needs. HRBE users also have the availability of an export capability to Excel, where they can store exported information locally.

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, HRBE does not use data to create predictive patterns or anomalies in searches, queries, or electronic databases. Furthermore, the results generated by the HRBE application are not designed to create or alter existing data elements/records.

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

Yes, currently the following DHS customers have assigned roles in HRBE: ICE, USCIS, NPPD, and DHS Headquarters (see Appendix A).

HRBE does not co-mingle information among CBP and its customers. Component information is segregated and only used within a specific component through a custom role-based security architecture. HRBE has delegated authority to each participating component to define their roles within each function of the component boundaries.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that HRBE users are able to export information from HRBE into Excel and store the information on local hard drives or shared drives.

Mitigation: This risk is partially mitigated, however there is currently no technical solution to prevent exports from HRBE. HRBE users are instructed in the proper use and security of HRBE records. Users are required to pass the annual Security Awareness, Privacy, and Rules of Behavior training to educate them in the protection of information and information systems. Individuals who violate the rule of behavior are subject to disciplinary action.

Privacy Risk: There is a risk to data minimization because HRBE maintains records about individuals who have been selected for positions within CBP but do not on-board due to various reasons including failure to pass medical, fitness, or background investigation tests.

Mitigation: This risk is partially mitigated. HRBE retains information on selected applicants who do not on-board in the event they re-apply for a position with CBP or appeal the results of their fitness, medical, or drug tests, or background investigations. Without additional applications or contested test results, no further information is created about these individuals and the records are purged after three years of inactivity.

Privacy Risk: There is a risk to data minimization that HRBE uses SSN and truncated SSN for several business functions.

Mitigation: Due to the high-volume, bulk hiring that CBP often conducts for CBP Officer and Agent positions at various times throughout the year, HRBE uses and displays SSN to de-conflict between applicants or employees with identical names. This is critical when ordering pre-employment tests such as a medical examinations, drug tests, or background investigations.

To minimize the privacy risk of data minimization, HRBE truncates SSN whenever displayed. In addition, each HRBE user has been properly vetted with security investigations and/or clearances; received the appropriate security and privacy training; access is only provided to those that have an authorized need to know in order to fulfill their position responsibilities; and in accordance with DHS policy, any misuse or improper access to data is met with sanctions and accountability.

Privacy Risk: The information in HRBE may be used for purposes outside the purpose for which it was collected.

Mitigation: DHS provides users with initial and annual refresher training in the form of Security Awareness, Privacy, and Rules of Behavior training to educate them in the protection of information and information systems. In accordance with policy, users complete this training within twenty-four hours of being granted a user account within their respective organizations; and this training informs users about their responsibilities for accessing and using information for "official" DHS reasons, and concerning the principles of "need to know." All HRBE users undergo training prior to accessing HRBE. If a user is performing questionable or inappropriate actions within HRBE, audit events will capture and track those actions and provide artifacts for analysis; thus presenting investigative factors to validate whether the actions taken by the user were inappropriate or if there was a valid business reason for the actions. Such

incidents will be reported to the user's supervisor, the Component Security Operations Center (SOC) and/or the Computer security Incident Response Capability (CSIRC), and access to HRBE will be revoked.

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.

This PIA provides notice to the individuals whose information is collected and maintained in HRBE. However in many cases, HRBE is not the initial point of collection. In these cases, notice is provided at the time of the collection by the source system/agencies via Privacy Act statements, which are included on all forms where required. These statements are available on websites, such as USAJOBS.gov website, as well as on the forms that are completed by the individuals, such as background investigations, security clearance checks, and financial disclosures.

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

The extent to which the individual may consent, decline, or opt out will vary with the HRBE function. Applicants are also given the opportunity to decline to provide their own information by not submitting their information for the employment opportunity. Some requested information is voluntary and an employee or applicant can decline to provide it. Declining to provide their information means that the individual chooses not to participate in the hiring process for that employment opportunity.

Newly hired employees are also given the opportunity to decline to provide their own information, or to opt to participate in only benefit programs of their choosing. Declining to provide their information will prevent the new hire employee from enrolling in that benefit program.

DHS employees also have the opportunity to decline to provide information requested. However, failure to provide certain items of information or comply with required drug testing, financial disclosure, performance plans, background investigations, etc. may affect benefits, rights, and employment. In addition, failure to provide requested information may delay the process of delivering benefits and personnel actions to the individual, because it might increase the time necessary to identify the individual and verify that the individual is authorized to receive the benefits. Also, the regulations at 5 CFR Part 2634 require employees designated as confidential filers to file new entrant and annual OGE Form 450 Confidential Financial Disclosure Reports.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is the risk that individuals were not provided notice prior to the collection of their information.

Mitigation: Applicants and employees are provided notice through the various related Privacy Act

SORNs and this PIA. In many cases, CBP is not the initial point of collection. When the point of initial collection is outside DHS, the agency collecting or requiring the information, such as OPM, DOL, or OGE provides a Privacy Act Statement on forms or online applications prior to the individual providing the information. These statements allow the individual to determine if he or she would like to submit the information. Additionally, applicants and employees are notified that references and other third parties may be consulted regarding employment qualifications candidates have provided or during background investigations.

If not immediately aware of HRBE upon entry into CBP, employees are fully aware once they are required to enter their information into HRBE. However in cases such as disciplinary situations, individuals may not be aware that this information is in HRBE until later in the disciplinary process. Background investigation and internal affairs information may not be subject to the Privacy Act notice requirement because JICMS is considered a law enforcement system, and providing notice could interfere with law enforcement investigations.

Section 5.0 Data Retention by the project

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

Record retention and disposal schedules vary by the type of record maintained and the official custodian of the record. Each of these record types has its own NARA-approved retention and disposal schedule, which can be found in the governing SORN (see Section 1.2). A comprehensive list of retention schedules by general HR category and SORN coverage can be found in Appendix C.

Although HRBE resides within CBP, OPM remains the official custodian for the majority of the personnel records maintained in HRBE including, but not limited to applicant records and federal employees' Electronic Official Personnel Folder (eOFP). Applicant records related to the hiring process are generally retained for three years. DOL Workers' Compensation Cases can be destroyed five years after the case is closed, whereas the record retention schedule for general personnel records is as follows:

The Official Personnel File (OPF) is maintained for the period of the employee's service in the agency and is then, if in a paper format, transferred to the National Personnel Records Center for storage, or as appropriate, to the next employing federal agency. If the OPF is maintained in an electronic format, the transfer and storage is in accordance with the OPM-approved electronic system. Other records are either retained at the agency for various lengths of time in accordance with the National Archives and Records Administration records schedules or destroyed when they have served their purpose or when the employee leaves the agency. The transfer occurs within 90 days of the individual's separation. In the case of administrative need, a retired employee, or an employee who dies in service, the OPF is sent within 120 days. Destruction of the OPF is in accordance with General Records Schedule-1 (GRS-1) or GRS 20.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: Because HRBE maintains so many different types of records, there is a risk that HRBE may retain records longer than necessary to fulfil the purpose of the specific function.

Mitigation: This risk is not mitigated. CBP does not automatically audit or monitor HRBE the lifecycle of records maintained within HRBE. Review depends on the continual monitoring and audits performed by the Business Process Solutions Division owner using reports. HRBE has been operational for six years and has not deleted any records.

Recommendation: The DHS Privacy Office requires that the HRBE program manager, in coordination with the CBP Privacy and Diversity Office, evaluate all functions within HRBE and develop record retention and deletion functionality consistent with the applicable records schedules described in Appendix C.

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.

Yes, HRBE shares information with other federal agencies, such as USDA and OPM, and private sector entities, such as CHS, through contract vehicles, including Interagency Agreements (IAAs) for the following purposes:

- HRBE shares daily information with the USDA via FTP to record, process, pay, and report personnel and payroll information for DHS employees.
- HRBE manually shares information with OPM on a daily basis to initiate a background investigation record used to determine suitability for employment.
- HRBE shares daily information with a private sector contractor (currently, CHS) to schedule drug, medical, and/or fitness tests. Data is transferred from HRBE via a manual upload to a SSL/TLS Portal.
- To the extent necessary, HRBE may share information with entities outside DHS as part of the following functions:
    - The Equal Employment Opportunity Commission (EEOC) or Merit Systems Protection Board (MSPB), as appropriate, for grievance proceedings, Equal Employment Opportunity (EEO) complaints, adverse actions, and mediation counseling sessions;
    - DOL OSHA in connection with safety inspections conducted; and
    - DOL for worker's compensation cases.
- Additionally, aggregated data may be shared for the purposes of published statistics and studies.

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

Information collected and maintained in HRBE may be shared outside DHS in accordance with the routine uses listed in each governing SORN, and routine uses may vary from SORN to SORN. Routine uses in each published SORN are compatible with the overall purpose for collection, which is different for each SORN. Nevertheless, data that is collected from contractors, employees, and applicants is shared only for purposes that directly support employment functions, including: the payment of salaries, background investigations, and for studies of personnel. Information maintained in the system may also be used to enforce employment rights through EEO and MSPB processes. For specific coverage and a more extensive descriptions of these routine uses, see the governing SORN for the specific function (see Section 1.2).

Any information disclosed outside of CBP is first reviewed and approved by the CBP Privacy and Diversity Office to ensure compatibility and to track external disclosures.

6.3 Does the project place limitations on re-dissemination?

Yes. All information collected, maintained, used, and disseminated from HRBE is covered by the Privacy Act. As such, information may only be disseminated consistent with the routine uses in the governing SORN and existing sharing agreements, when applicable. CBP and its customers do not share information externally in a manner inconsistent with these Privacy Act protections.

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

Information exchanged between HRBE and the external entities described in Section 6.1 are conducted through various file exchange methods. These file exchanges are established through sharing agreements and monitored daily through established exchange procedures and automated auditing tools within HRBE. HRBE captures the date(s) when information is sent and received and maintains detailed logs of these events. The HRBE auditing tools are designed to ensure appropriate user access, detect intrusions, create audit trails, and identify problems. Audit trails are periodically reviewed by system personnel, and preserved as required by the applicable record retention schedule. Suspected or confirmed security or privacy issues are elevated to system security and management, as appropriate.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that information shared outside HRBE will be shared externally for a purpose inconsistent with the sharing agreement and the governing SORN.

Mitigation: All information collected, maintained, used, and disseminated from HRBE may only be shared consistent with the sharing agreement and the routine uses in the governing SORN. CBP and its customers do not share information externally in a manner inconsistent with these Privacy Act protections. This risk is further mitigated because the information maintained in HRBE is limited to necessary information and only shared with those entities who have an official need to know.

Section 7.0 Redress

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

During the hiring and on-boarding process, individuals have the ability to access and change their own profiles within USAJOBs and Application Manager at any time. Applicants are made aware at the time that they receive their login information that they may correct or update any erroneous information that may have been submitted prior to the application being processed or the expiration of the employment opportunity. Privacy Act notices are also posted on personnel forms and applications during each stage of the hiring process. Hired employees are able to access and view personnel file actions in their eOPF.

In addition, individuals seeking notification of and access to any CBP record contained in HRBE or to seek corrections, pursuant to procedures provided by the Freedom of Information Act (FOIA)[30] and the access provisions of the Privacy Act of 1974 with CBP at https://www.cbp.gov/site-policy-notices/foia, or by mailing a request to:

U.S. Customs and Border Protection (CBP)
Freedom of Information Act (FOIA) Division
90 K Street, NE
Washington, DC 20229

Individuals seeking notification and access to records contained in HRBE but owned by another DHS component, need to contact the FOIA office for that DHS component. Although CBP owns HRBE, each DHS customer maintains ownership of its own data and therefore, controls the disclosure of that data. If CBP receives a FOIA or Privacy Act request for information within HRBE that belongs to a customer component, CBP will refer the FOIA or Privacy Act request to that DHS component.

When seeking records about yourself from this system of records or any other Departmental system of records, your request must conform to the Privacy Act regulations set forth in federal regulations regarding Domestic Security and Disclosure of Records and Information.[31] You must first verify your identity, meaning that you must provide your full name, current address, and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under federal statute regarding Unsworn Declarations Under Penalty of Perjury,[32] a law that permits statements to be made under penalty of perjury as a substitute for notarization. While your inquiry requires no specific form, you may obtain forms for this purpose from the Chief Privacy Officer and Chief Freedom of Information Act Officer, https://www.dhs.gov/freedom-information-act-foia or 1-866-431-0486. In addition, you should:

- Explain why you believe the Department would have information on you;

[30] 5 U.S.C. § 552.
[31] 6 CFR Part 5.
[32] 28 U.S.C. § 1746; *available at* http://www.gpo.gov/fdsys/pkg/USCODE-2011-title28/pdf/USCODE-2011-title28-partV-chap115-sec1746.pdf.

- Identify which component(s) of the Department you believe may have the information about you;
- Specify when you believe the records would have been created; and
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records.

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

Individuals may correct inaccurate or erroneous information in HRBE by following the procedures described in Section 7.1.

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

Through the publication of this PIA, individuals seeking notification of and access to any record contained in HRBE are informed that they may submit a request through the procedures in 7.1 and 7.2, above. Individuals also receive notice via the governing SORNs described in Section 1.2.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a privacy risk that individuals may file a FOIA or Privacy Act request with CBP for information stored in HRBE but owned by other DHS components, which may lead to an inappropriate denial of a legitimate FOIA or Privacy Act request, or a lengthy delay

Mitigation: To mitigate this risk, CBP FOIA staff must refer such individuals to the DHS FOIA office that maintains the requested records. Given the segregation of information by component within HRBE, CBP FOIA would not be an appropriate source to obtain data belonging to another component.

Privacy Risk: There is a privacy risk that applicants and employees will not be able to access, correct, or amend their personnel records.

Mitigation: All Government personnel records are covered by the Privacy Act and fall under the SORN governing that particular function, typically without any Privacy Act exemptions. There are Privacy Act notices on all OPM applications and DHS IT systems/application management systems to alert applicants and employees that their records are afforded Privacy Act protections. In addition, the Government–wide eOPF system displays personnel actions taken on behalf of the employee. And in addition to the associated SORNs, this PIA also provided information concerning the access and correction of information within HRBE.

For internal affairs or investigatory records, individuals may be unable to access their personnel records if related to an active investigation or pursuant to a Privacy Act exemption.

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?

HRBE has implemented security controls and technology features that incorporate protection of privacy; complies with FISMA and NIST protocols and procedures, and mitigates privacy risks. HRBE ensures that the information is used in the manner for which it was designed by:

- Protecting sensitive information such as hard copy media, backup media, and removable media in a secure location, such as locked: offices, rooms, desks, bookcases, file cabinets, or other storage mechanism to prohibit access by unauthorized individuals; labeling media with "Sensitive-But-Unclassified (SBU)" or "For Official Use Only (FOUO)" as appropriate to safeguard against unauthorized disclosure, modification, access, use, or destruction; and sanitizing media by destroyed by shredding, burning, pulping, or pulverizing copies containing PII.
- Creating audit logs of identified events containing: users, date, time, and action taken to provide an overall accounting of events, to support "after the fact" investigations of security incidents, and retaining that data throughout the lifecycle of the application.
- Monitoring the security controls that focus on, review, and assess specific controls (account management, audit record content, non-repudiation, user identification and authentication, security categorization, vulnerability scanning, boundary protection, transmission integrity/confidentiality, protection of information at rest, and security functionality verification) to ensure that the application is secure and operating as intended.
- Enforcing user roles through Identity, Credential, and Access Management (ICAM)[33] for CBP users and Microsoft Active Directory (AD)[34] for other DHS customers to restrict rights/privileges or access by users to official need to know. HRBE applies the principle of least privilege to the user community. However, once a user is validated, HRBE grants rights based upon need to know to each participating component to define their roles within each function of the component boundaries
- HRBE undergoes a security authorization every three years in which security testing and evaluation is conducted by an independent party. In addition, the HRBE application undergoes an annual self-assessment to ensure the required security levels are being maintained.

[33] DHS/ALL-004 Department of Homeland Security/ALL-004 General Information Technology Access Account Records System of Records, November 27, 2012, 77 FR 228, *available at:* https://www.gpo.gov/fdsys/pkg/FR-2012-11-27/html/2012-28675.htm and DHS/ALL-037 e-Authentication, August 11, 2014, 79 FR 46857, *available at:* https://www.gpo.gov/fdsys/pkg/FR-2014-08-11/html/2014-18703.htm.
[34] DHS/ALL/PIA-012(b) E-Mail Secure Gateway, January 14, 2009, *available at:* https://www.dhs.gov/sites/default/files/publications/privacy_pia_dhs_dses_0.pdf

- HRBE has measures in place that provide audit traces of performed activity. For instance, if a HR Specialist reviews his/her own information, there are audit trails in place that would identify that type of behavior and the frequency with which it is occurring.

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

CBP users are required to take CBP Security Awareness classes on an annual basis. CBP users also may be required to take: TECS Privacy Awareness (TPA), General Privacy Awareness (GPA), and Security Awareness Training. Training classes based upon job classification. Completion of these course is tied to CBP user access. In addition, role-based training is provided in the form of CBP Privileged User Training and System Owner Training.

If refresher training is not completed within a one (1) year timeframe, CBP user access is revoked, thereby revoking access to the HRBE application.

At a minimum, other DHS components are required to comply with DHS-wide privacy training requirements, as well as any additional requirements established by each component as a condition for HRBE access.

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

HRBE uses role-based access controls that are employed to limit the access of information by different users and administrators based on the principles of segregation of duty and least privilege through an authorized need to know.

Specified HRBE users are allowed remote access to the application through encrypted communication and two-factor authentication.

HRBE users are Government employees and/or Government-contracted employees in CBP, ICE, NPPD, and DHS HQ. HRBE users are categorized as "general" or "administrative" users. General users only access the functionality within the HRBE application via the web interface, and are either HR professionals or administrative personnel. Administrative users are application administrators and security personnel. The following user roles are supported within the HRBE application:

- Administrators – administer rights and privileges to system capabilities and content;
- HR Analysts/Specialists – read and execute content made available by content authors for the specific HRBE Function(s) they are given access to; and
- Developers – develop application metadata models to support content.

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?

At a minimum, DHS components submit a signed Interagency Agreement (IAA) Agreement Between Federal Agencies, and a Statement of Work outlining the Scope, Task Requirements, Deliverables, Security Requirements and Period of Performance to CBP's Office of Human Resources Management to obtain HRBE services.

The policy for connecting non-CBP systems requires that the non-CBP portion meet or exceed the protection requirements enforced by CBP. Organizations must have a signed Interconnectivity Security Agreement (ISA) in place prior to connecting with CBP.

Responsible Officials

Steven Stryk
Office of Human Resources Management (HRM)
Business Process Solutions Division (BPS)
U.S. Customs and Border Protection

Debra L. Danisek
Acting Privacy Officer
Office of Privacy and Diversity
Office of the Commissioner
U.S. Customs and Border Protection

Approval Signature

Original signed copy on file with the DHS Privacy Office.

_____

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

APPENDIX A
HRBE Functions Used by Other DHS Components

Component	Function Access
DHS Headquarters	Financial Disclosure OGE-450 Function Ticketing
ICE	Entry and Professional Level Hiring Employee Relations Labor Relations Ticketing
USCIS	Employee Relations Labor Relations Ticketing
FEMA[35]	Financial Disclosure OGE-450 Function
NPPD	Financial Disclosure OGE-450 Function

[35] In April 2018, FEMA was added to the list of DHS Components in Appendix A of this PIA, to document the agency's use of HRBE for the Financial Disclosure/OGE-450 reporting function. FEMA's permissions in HRBE are identical to those of the other components (ICE, NPPD & USCIS) who use HRBE.

APPENDIX B
Level of Access by HRBE Function

	Function	Roles	Role Description
1	**Performance Management (PM)**	PM_Admin	Administers the performance management workflow. They are able to assign additional roles to users and take action on behalf of employees on their performance plans
		PM_Agency_Goal	Allows the users to edit Agency level performance goals
		PM_DHS_Goal	Allows users to edit DHS level performance goals
		PM_Employee	This role grants users access to the performance management workflow as a federal employee able to receive performance plans.
		PM_POC	The organization point of contact. This user is able to act as an employee and perform administrative tasks on his/her performance plans but only within his/her own organization level and below
		PM_Prog_Office_Goal	Allows this user to edit the program office level performance goals
		PM_Rating_Official	This role grants the user access as a federal supervisor able to issue performance plans to his/her direct reports and rate their performance
		PM_Super_POC	This role is the same as the POC role but is granted at the program office level.

Function		Roles	Role Description
			This user is able to perform POC-like tasks for the whole program office
		PM_User_Reports	Allows this user to run reports
		PM_View_Only	Allows user to view/search performance plans but not take any action
2	**Entry and Professional Level Hiring**	Hiring Entry Level	Access to the Entry Level tracking system
		User Administrator	Allows user to administer roles in Entry and Professional Hiring
		Fitness Results	Allows access to enter detailed fitness results into the system
		Email PFT2	Allow the sending of emails to applicants regarding the second physical fitness test.
		Email Refer to Scheduling and EOD	Allow the sending of emails to applicants regarding academy scheduling and EOD information.
3	**Senior Executive Service (SES)**	SATS_User	Allows user full user / admin access to Senior Executive Service hiring workflow
4	**Table of Organization**	TO_User	Allows user access to set organizational targets at specific levels or his/her own organization
		TO_Super_User	Allows user access to set organizational targets for all organizations and all levels
		TO_Org_Target_User	Sets the high level program office targets
		TO_Admin	Allows user to add / remove users

	Function	Roles	Role Description
5	**Safety Inspection**	STAR_View_only	View-only access to search and open inspection reports
		STAR_Supervisor	Allows user to perform a review of the safety inspections before it is sent to the building management
		STAR_Safety_Specialist	Users performing the safety inspections
		STAR_MSS	Mission Support Specialist runs reports and manages the overall process and acts as a liaison between safety specialists and the building management.
		STAR_MOIC_Reporting	Management Official In Charge (MOIC) is the building management in charge of remediating all the safety findings
		STAR_Health_Physicist	Users performing inspections on the radiation equipment at CBP facilities
		STAR_Email_Admin	Users allowed to modify email templates that are used to send emails in the workflow
		STAR_Delegate	Users delegated responsibility to remediate safety finding by the MOIC
		Star_Admin	Allows user to administer roles, facilities, standard findings
6	**Employee Relations (ER)**	Assigned_DRB_Supervisor (Discipline Review Board)	Allows DRB supervisor assigned to case to perform supervisory actions
		Assigned_DRB_Specialist	Allows DRB specialist assigned to case to perform workflow actions
		Assigned_Supervisor	Allows DRB supervisor to view case
		Assigned Labor and Employee Relations (LER)_Specialist	Allows LER specialist assigned to case to perform

Function		Roles	Role Description
			workflow actions
		Assigned_Intake_Specialist	Allows intake specialist assigned to case to perform intake review workflow actions
		Assigned_Intake_Assistant	Allows intake assistant assigned to case to perform intake workflow actions
		Agency_Intake_Assistant	Allows DRB intake assistant to view case within his/her agency at select stages
		Agency_Intake_Specialist	Allows DRB intake specialist to view case within his/her agency at select stages
		Agency_LER_Admin (Labor and Employee Relations)	Allows LER administrator to take select migration actions for cases within his/her agency
		Agency_DRB_Admin	Allows DRB administrator to take select migration actions for cases within his/her agency
		Agency_Specialists	Allows DRB specialist/DRB supervisor or LER specialist/LER supervisor to take select migration actions for cases within his/her agency
		LER_Specialist	Allows LER specialist to perform workflow actions
		LER_Supervisor	Allows LER supervisor to perform supervisory actions
		LER_Administrator	Allows LER administrator to perform actions taken by LER specialist/LER supervisor and administrative actions
		DRB_Specialist	Allows DRB specialist to perform workflow actions
		DRB_Supervisor	Allows DRB supervisor to

Function		Roles	Role Description
			perform supervisory actions
		DRB_Administrator	Allows DRB administrator to perform actions taken by DRB specialist/DRB supervisor and administrative actions
		DRB_Intake_Specialist	Allows DRB intake specialist to perform select actions
		DRB_Intake_Assistant	Allows DRB intake assistant to perform select actions
		HRBE_Admin	Allows access to admin form to load cases
		ER_Dashboard	Allows access to ER dashboard (external interface)
		ER_QueryStudio	Allows access to ER Query Studio (external interface)
		ER_Analysis	Allows access to ER Analysis Studio (external interface)
		ER_Super_Maintenance	Allows access to admin forms to update critical fields or delete cases
		ER_DD_Administrator (Discipline Dashboard)	Allows access to admin form to manage discipline dashboard users
		ER_DD_Org_Level_2_User	Allows access to specified CBP level 2 org data in discipline dashboard
		ER_DD_Org_Level_3_User	Allows access to specified CBP level 3 org data in discipline dashboard
		ER_DD_CBP	Allows access to CBP data in discipline dashboard
7	**Fitness**	PFT2_User	Allows user to enter fitness results
		PFT2_admin	Administers the user roles for fitness workflow
8	**Labor Relations**	Assigned_LR_Specialist	Allows specialist assigned

	Function	Roles	Role Description
	(LR)		to the case to perform workflow actions
		LR_Super_Maintenance	Allows access to admin forms to update critical fields or delete cases
		Assigned_LER_Supervisor	Allows assigned specialist's team supervisor to perform supervisory actions
		Agency_LR_Supervisor	Allows supervisor to perform supervisory actions for cases within his/her agency
		HRBE_LR_Supervisor	Allows supervisor to perform supervisory actions
		HRBE_LR_Specialist	Allows specialist to perform workflow actions
		HRBE_LR_Admin	Allows access to administrative forms and actions
		HRBE_LR_QueryStudio	Allows access to Query Studio (external interface)
		HRBE_LR_Dashboard	Allows access to LR dashboard (external interface)
		HRBE_LR_AnalysisStudio	Allows access to Analysis Studio (external interface)
9	**Drug Free Workplace (DFWP)**	Administrator	Can do all things the specialist can do but also has the ability to maintain users, tables, regions and explicit lists
		Specialist	General user of the DFWP tool. Can perform all non-administrative functions
10	**Financial Disclosure OGE-450**	Filer	Allows user to be a OGE450 filer
		Final Approver	User performs the final approval for OGE450 filings

	Function	Roles	Role Description
		Designee	User designated by final approver to perform the final approval
		POC	Point of contact can monitor and take administrative action on OGE450 filing within their organization
		Program Office Admin	User, also known as the Organizational Admin, can administer filings at the program office level
		Supervisor	User performs the supervisor approvals for filings
		Viewer	Allows user to search and view filings
		Report Analysis	Allows user to access Cognos analysis studio
		Report Query	Allows users to access Cognos Query Studio
		Report Dashboard	Allows user to access the financial disclosure dashboard in Cognos
11	**Customer Inquiry Tracking (CIT)**	AssignedUser	Places case folder on the to-do list of the current assigned user
		CIT_Admin	Global admin user access to all blank/admin forms
		CIT_FAQ_Supervisor	FAQ process supervisor approves FAQ requests
		CIT_Initiators	Users that can start requests
		CIT_Super_Maintenance	Super users that maintain topics/subtopics/teams
		CIT_Supervisor	Supervisors that oversee and resolve tickets
		CIT_Supervisor_Administration	Access to admin forms
		CIT_Tier1	Users belonging to designated Tier 1 team
		CIT_Tier2	Users belonging to designated Tier 2 team
		CIT_Tier3	Users belonging to

	Function	Roles	Role Description
			designated Tier 3 team
12	**Retirement Tracking (RT)**	RT_Management	Users who initiate RT, update case, reassign case, view RT archived package search form, view RT Reports
		RT_Worker	Users who initiate RT, audit processed case, update case, reassign case, view RT archived package search form
		RT_Assistant	Users who initiate RT, update case, reassign case, view RT reports
		RT_Specialist	Users who initiate RT, pool of specialist for assignment, reassign case, view RT
		RT_Assigned_Specialist	Users who assigned specialist for a case, view RT Reports
		RT_UserMaintenance	Users who access retirement tracking administration form, view RT archived package search form, view RT reports
13	**Background Investigations (BI)**	BI Supervisor	Users with full access to the module
		BI Specialist	Users with full access to the module
		BI Assistant	User who performs most actions, except ones that need higher levels of authority, such as returns from IA (Internal Affairs)
		BI Observer	User with view-only in Module, but performs no actions
		BI Administrator	User who has full access to the Module, including the admin forms for data set up

Function		Roles	Role Description
		BI SSN Viewer	Users who can see the full SSN, and not just the four digits
		BI Academy Report	Users with access to the IA Academy Report
		BI Metrics Report	Users with access to the BI metrics report
14	**Personnel Action Request**	SF52_Create	All users who can create SF-52 request
		SF52 Org Submitter (Lvl 1 Approver)	Users who can submit SF-52. Cannot be person named as employee on SF-52
		SF52_CurrentApprovalTier	Users who have sign ability for current approval level
		SF52_HigherApprovalTier	Users who have sign ability higher than current level
		SF52_OrgAdm	Administrators within specific organization. Can send notifications, reassign requests, and revoke roles
		SF52_SysAdm	Administrators with general access to all functions within the process.
		SF52_User	All users with any role regardless of organization
		SF52_Copy	Create/Sign users with access to Organization
		SF52_Level2OrgAdm	Level 2 Organization Administrators who can set who has sign ability used in the approval tiers for submission of requests
		SF52_HRTeamMember	Specific HR Team member assigned to request
		SF52_HRTeam	All members of team assigned to request
		SF52_HRPayApprovers	Any HR user with Pay Approve authority (within Agency)
		SF52_HRFinalApprovers	Any HR user with Final Approve authority (within

Function		Roles	Role Description
			Agency)
		SF52_HRUser	Member of any HR team within agency
		SF52_HRAdmin_Agency	Agency-Specific HR Administrators
		SF52_HRViewer	Member with Any HR role within agency
		SF52_HRAdmin_FormList	HR Admins in any agency (For Form List)
		SF52_HRTransmitter	Any HR user with transmit authority (within Agency)
		SF52_HRClassApprover	Any HR user with Class Approve authority (within Agency)
		SF52_HRTeamForAdminForms	Not agency aware - cannot be since no agency declared yet
		SF52_HRViewer_NoAgency	Not agency aware - member with any HR role
		SF52_Mass_BusinessOwner	Action-Specific Owners/Administrators for a given type of Mass Process – i.e., Organization Design Division (ODD) does Realignments
		SF52_Mass_ProgramOfficeToDo	Defined by Business Owners in the Task form who have active items to do
		SF52_Mass_ProgramOffice	Defined by Business Owners in Task Form - no Active Task assigned
		SF52_MassSearch_Access	Business Owners and Program Office
		SF52_Mass_Owners	Business Owners who can start Mass Process
		SF52_Mass_OrgAdmins	Org Admins for orgs included in the particular requests realign list
15	**Medical and Contracting Officer's Representative**	Med Supervisor	User with full access to the Med Module

	Function	Roles	Role Description
		Med Specialist	User with full access to the Med Module
		Med Assistant	User who can perform most actions, except ones that need higher levels of authority, and cannot make any decisions on the cases: Cleared, Failed to Respond, Disqualified, and Insufficient
		Med Observer	User with view-only in the Module, but performs no actions
		Med Administrator	Administrator with full access to the Med Module, including the admin forms for data set up
		Med Nurse	Nurse who can only evaluate the medical part of the module: Exams, Consults, Follow Ups
		Med Manual	User who can manually start a case, or enter web service data with this role
		Med SSN Viewer	User who can to see the full SSN, and not just the four digits
		COR Administrator	Administrator who has full access to the Module, including the admin forms for data set up
16	**Employee Position Profile**	Employee_Profile_Admin	Administrator who has read-write access to all forms
		Employee_Profile_Data_Elements	User who has read-write access to the position/person data elements admin forms
		Employee_Profile_HR_Viewer	User who has view only forms access for employee/position data
		Employee_Profile_MRN_Lookup	Use who has read-access to

	Function	Roles	Role Description
			Master Record Number (MRN) data
		Employee_Profile_Person_Lookup	User who has read-access to person lookup form
		Employee_Profile_Reports_Viewer	User with access to reports
		Employee_Profile_Role_Admin	Designated Role Administrator who can grant workflow access permissions to users
17	**Ticketing**	HRBE_Issue_Tracking_UI_Team	Business Process Solutions (BPS) User Interface (UI) Team for workflow task assignment
		HRBE_Issue_Tracking_Tier_1	Client Tier 1 support users responsible for reviewing tickets submitted and testing in SAT environment
		HRBE_Issue_Tracking_Submitter	Users authorized to submit a ticket
		HRBE_Issue_Tracking_SAFR_Team	BPS Simulation Accountability Feedback and Reporting (SAFR) Team for workflow task assignment
		HRBE_Issue_Tracking_Reassign	Users authorized to reassign a ticket
		HRBE_Issue_Tracking_Product_Mgr	Designated Product Managers
		HRBE_Issue_Tracking_PM	BPS PM Team for workflow task assignment
		HRBE_Issue_Tracking_LOE	Users responsible for doing Level of Effort estimates
		HRBE_Issue_Tracking_LAN_Support	BPS LAN Support Team for workflow task assignment
		HRBE_Issue_Tracking_ISSO_Team	BPS ISSO Team for workflow task assignment
		HRBE_Issue_Tracking_DB_Team	BPS DB Team for workflow task assignment
		HRBE_Issue_Tracking_CPRO_Team	BPS Consolidated Personnel Reporting Online (CPRO) Team for

Function		Roles	Role Description
			workflow task assignment
		HRBE_Issue_Tracking_Comms_Team	BPS Communications Team for workflow task assignment
		HRBE_Issue_Tracking_Admin	Users designated as the overall ticketing administrators
		Business_Justification	Users responsible for doing business justifications for enhancements
		Agency_Category_Changer	Allowed to change agency category for a ticket

APPENDIX C
Record Retention Schedule by Category and SORN Coverage

	Basic Record Category	SORN	Record Retention Schedule
1	**Personal Actions and Records**	OPM/GOVT-1 General Personnel Records[36] SORN	The Official Personnel File (OPF) is maintained for the period of the employee's service in the agency and is then, if in a paper format, transferred to the National Personnel Records Center for storage or, as appropriate, to the next employing Federal agency. If the OPF is maintained in an electronic format, the transfer and storage is in accordance with the OPM approved electronic system. Other records are either retained at the agency for various lengths of time in accordance with the National Archives and Records Administration records schedules or destroyed when they have served their purpose or when the employee leaves the agency. The transfer occurs within 90 days of the individuals' separation. In the case of administrative need, a retired employee, or an employee who dies in service, the OPF is sent within 120 days. Destruction of the OPF is in accordance with General Records Schedule-1 (GRS-1) or GRS 20. Records contained within the Central Personnel Data File (CPDF) and Enterprise Human Resource Integration (EHRI) (and in agency's automated personnel records) may be retained indefinitely as a basis for longitudinal work history statistical studies. After the disposition date in GRS-1 or GRS 20, such records should not be used in making decisions concerning employees.
		OPM/GOVT-2 Employee Performance File System Records[37] SORN	Records on former non-SES employees will generally be retained no longer than 1 year after the employee leaves his or her employing agency. Records on former SES employees may be retained up to 5 years under 5 U.S.C. 4314. a. Summary performance appraisals (and related records as the agency prescribes) on SES appointees are retained for 5 years and ratings of record on other employees for 4 years, except as shown in paragraph b. below, and are disposed of by

[36] OPM/GOVT-1 General Personnel Records (December 11, 2012), 77 FR 73694, *available at:* https://www.gpo.gov/fdsys/pkg/FR-2012-12-11/html/2012-29777.htm.
[37] OPM/GOVT-2 Employee Performance File System Records (June 19, 2006), 71 FR 35342, *available at:* https://www.gpo.gov/fdsys/pkg/FR-2006-06-19/html/06-5459.htm.

	Basic Record Category	SORN	Record Retention Schedule
			shredding, burning, erasing of disks, or in accordance with agency procedures regarding destruction of personnel records, including giving them to the individual. When a non-SES employee transfers to another agency or leaves federal employment, ratings of record and subsequent ratings (4 years old or less) are to be filed on the temporary side of the OPF and forwarded with the OPF. b. Ratings of unacceptable performance and related documents, pursuant to 5 U.S.C. 4303(d), are destroyed after the employee completes 1 year of acceptable performance from the date of the proposed removal or reduction-in-grade notice. (Destruction to be no later than 30 days after the year is up.) c. When a career appointee in the SES accepts a Presidential appointment pursuant to 5 U.S.C. 3392(c), the employee's performance folder remains active so long as the employee remains employed under the Presidential appointment and elects to have certain provisions of 5 U.S.C. relating to the Service apply. d. When an incumbent of the SES transfers to another position in the Service, ratings and plans 5 years old or less shall be forwarded to the gaining agency with the individual's OPF. e. Some performance-related records (e.g., documents maintained to assist rating officials in appraising performance or recommending remedial actions or to show that the employee is currently licensed or certified) may be destroyed after 1 year. f. Where any of these documents are needed in connection with administrative or negotiated grievance procedures, or quasi-judicial or judicial proceedings, they may be retained as needed beyond the retention schedules identified above. g. Generally, agencies retain records on former employees for no longer than 1 year after the employee leaves.
		OPM/GOVT-3 Records of Adverse Actions, Performance Based Reduction in Grade and Removal Actions, and Termination of	Records documenting an adverse action, performance-based removal or demotion action, or covered actions against probationers are disposed of not sooner than four years nor later than seven years after the closing of the case in accordance with each agency's records disposition manual. Disposal is by shredding, or erasure of tapes (disks).

	Basic Record Category	SORN	Record Retention Schedule
		Probationers[38] SORN	
		OPM/GOVT-5 Recruiting, Examining, and Placement Records[39] SORN	Records in this system are retained for varying lengths of time, ranging from a few months to 5 years, e.g., applicant records that are part of medical determination case files or medical suitability appeal files are retained for 3 years from completion of action on the case. Most records are retained for a period of 1 to 2 years. Some records, such as: individual applications, become part of the person's permanent official records when hired, while some records (e.g., non-competitive action case files), are retained for 5 years. Some records are destroyed by shredding or burning while magnetic tapes or disks are erased.
		OPM/GOVT-6 Personnel Research and Test Validation Records[40] SORN	Records are retained for 2 years after completion of the project unless needed in the course of litigation or other administrative actions involving a research or test validation survey. Records collected for longitudinal studies will be maintained indefinitely. Manual records are destroyed by shredding or burning and magnetic tapes and disks are erased.
		OPM/GOVT-7 Applicant Race, Sex, National Origin and Disability Status Records[41] SORN	Records are generally retained for 2 years, except when needed to process applications or to prepare adverse impact and related reports, or for as long as an application is still under consideration for selection purposes. When records are needed in the course of an administrative procedure or litigation, they may be maintained until the administrative procedure or litigation is completed. Manual records are shredded or burned and magnetic tapes and disks are erased.
2	**Contractors and Consultants**	DHS/ALL-021 Department of Homeland	Records are retained for six years and three months after the final payment to a contractor/consultant in accordance with National Archives and Records Administration-approved

[38] OPM/GOVT-3 Records of Adverse Actions, Performance Based Reduction in Grade and Removal Actions, and Termination of Probationers (April 27, 2000), 65 FR 24732, *available at*: https://www.gpo.gov/fdsys/pkg/FR-2000-04-27/html/00-10088.htm.
[39] OPM/GOVT-5 Recruiting, Examining, and Placement Records (June 19, 2006), 71 FR 35351, *available at:* https://www.gpo.gov/fdsys/pkg/FR-2014-03-26/html/2014-06593.htm.
[40] OPM/GOVT-6 Personnel Research and Test Validation Records (June 19, 2006), 71 FR 35354, *available at:* https://www.gpo.gov/fdsys/pkg/FR-2006-06-19/html/06-5459.htm.
[41] OPM/GOVT-7 Applicant Race, Sex, National Origin and Disability Status Records (June 19, 2006), 71 FR 35356, *available at:* https://www.gpo.gov/fdsys/pkg/FR-2006-06-19/html/06-5459.htm.

	Basic Record Category	SORN	Record Retention Schedule
		Security Contractors and Consultants SORN[42]	General Records Schedule 3, Item 3--General Procurement Files.
3	**Employee Relations, Internal Affairs, and Professional Responsibility**	DHS/ALL-018 Department of Homeland Security Grievances, Appeals, and Disciplinary Action Records System of Records[43] SORN	Records are destroyed no sooner than 2 years but no later than 7 years after a case is closed, in accordance with National Archives and Records Administration General Records Schedule 1, Civilian Personnel Records, Item 30.
4	**Labor Relations Cases**	OPM/GOVT-9 File on Position Classification Appeals, Job Grading Appeals, Retained Grade or Pay Appeals, Fair Labor Standard Act (FLSA) Claims and Complaints, Federal Civilian Employee Compensation and Leave Claims, and Settlement of Accounts for Deceased Civilian Officers and Employees	Records related to position classification appeal, job grading appeal, retained grade or pay appeal files, FLSA claims or complaints, compensation and leave claims, or disputes concerning the settlement of the account for a deceased federal civilian officer or employees are maintained for 7 years after closing action on the case. Records are destroyed by shredding, burning, or erasing as appropriate.

[42] DHS/ALL-021 Department of Homeland Security Contractors and Consultants System of Records (October 23, 2008), 73 FR 63179, *available at:* https://www.gpo.gov/fdsys/pkg/FR-2008-10-23/html/E8-25205.htm.
[43] DHS/ALL-018 Department of Homeland Security Grievances, Appeals, and Disciplinary Action Records System of Records (October 17, 2008), 73 FR 61882, *available at:* https://www.gpo.gov/fdsys/pkg/FR-2008-10-17/html/E8-24741.htm.

	Basic Record Category	SORN	Record Retention Schedule
		File on Position Classification Appeals, Job Grading Appeals, and Retained Grade or Pay Appeals, and Fair Labor Standard Act (FLSA) Claims and Complaints[44] SORN	
		EEOC/GOVT-1 Equal Employment Opportunity in the Federal Government Complaint and Appeal Records[45] SORN	These records are maintained for one year after resolution of the case and then transferred to the Federal Records Center where they are destroyed after three years.
		DOL/GOVT-1 Office of Worker's Compensation Programs (OWCP), Federal Employees' Compensation Act File[46] SORN	All case files and automated data pertaining to a claim are destroyed 15 years after the case file has become inactive. Case files that have been scanned to create electronic copies are destroyed after the copies are verified. Electronic data is retained in its most current form only, and as information is updated, outdated information is deleted. Some related financial records are retained only in electronic form, and destroyed six years and three months after creation or receipt.
		OPM/GOVT-10	The Employee Medical Folder (EMF) is maintained for the

[44] OPM/GOVT-9 File on Position Classification Appeals, Job Grading Appeals, Retained Grade or Pay Appeals, Fair Labor Standard Act (FLSA) Claims and Complaints, Federal Civilian Employee Compensation and Leave Claims, and Settlement of Accounts for Deceased Civilian Officers and Employees File on Position Classification Appeals, Job Grading Appeals, and Retained Grade or Pay Appeals, and Fair Labor Standard Act (FLSA) Claims and Complaints (October 1, 2013), 78 FR 60331, available at:https://www.gpo.gov/fdsys/pkg/FR-2013-10-01/html/2013-23839.htmhttps:/www.gpo.gov/fdsys/pkg/FR-2013-10-01/html/2013-23839.htm.

[45] EEOC/GOVT-1 Equal Employment Opportunity in the Federal Government Complaint and Appeal Records (July 30, 2002), 67 FR 49338, *available at:* https://www.gpo.gov/fdsys/pkg/FR-2002-07-30/html/02-18895.htm.

[46] DOL/GOVT-1 Office of Worker's Compensation Programs, Federal Employees' Compensation Act File (January 11, 2012), 77 FR 1738, *available at:* https://www.gpo.gov/fdsys/pkg/FR-2012-01-11/html/2012-345.htm.

	Basic Record Category	SORN	Record Retention Schedule
		Employee Medical File System Records[47] SORN	period of the employee's service in the agency and is then transferred to the National Personnel Records Center for storage, or as appropriate, to the next employing federal agency. Other medical records are either retained at the agency for various lengths of time in accordance with the National Archives and Records Administration's records schedules or destroyed when they have served their purpose or when the employee leaves the agency. Within 90 days after the individual separates from the federal service, the EMF is sent to the National Personnel Records Center for storage. Destruction of the EMF is in accordance with General Records Schedule-1(21). Records arising in connection with employee drug testing under Executive Order 12564 are generally retained for up to 3 years. Records are destroyed by shredding, burning, or by erasing the disk.
		DHS/ALL-022 Department of Homeland Security Drug Free Workplace[48] SORN	Records are destroyed after three years, in accordance with National Archives and Records Administration General Records Schedule 1, Item 36.
5	**General System Access**	DHS/ALL-004 General Information Technology Access Account Records System (GITAARS)[49] SORN	Records are securely retained and disposed of in accordance with the National Archives and Records Administration's General Records Schedule 24, section 6, ``User Identification, Profiles, Authorizations, and Password Files." Inactive records will be destroyed or deleted 6 years after the user account is terminated or password is altered, or when no longer needed for investigative or security purposes, whichever is later.
6	**Customer Inquiries, Comments and**	DHS/ALL-016 Department of Homeland Security	Executive-level records are permanent, and files are cut off annually and transferred to the National Archives and Records Administration 10 years after cut-off date, in accordance with National Archives and Records Administration General

[47] OPM/GOVT-10 Employee Medical File System Records (June 21, 2010), FR 73694, *available at:* https://www.gpo.gov/fdsys/pkg/FR-2010-06-21/html/2010-14838.htm.
[48] DHS/ALL-022 Department of Homeland Security Drug Free Workplace (October 31, 2008), 73 FR 64974, *available at:* https://www.gpo.gov/fdsys/pkg/FR-2008-10-31/html/E8-25971.htm.
[49] DHS/ALL-004 General Information Technology Access Account Records System (GITAARS) (November 27, 2012), 77 FR 70792, *available at:* https://www.gpo.gov/fdsys/pkg/FR-2012-11-27/html/2012-28675.htm.

	Basic Record Category	SORN	Record Retention Schedule
	Complaints	Correspondence Records[50] SORN	Schedule N1-563-07-13-4 (Pending NARA Approval). Non-executive level records are destroyed after 10 years, in accordance with a pending National Archives and Records Administration General Records Schedule.
7	**Ethics Programs and Financial disclosures**	OGE/GOVT-1 Executive Branch Personnel Public Financial Disclosure Reports and Other Name-Retrieved Ethics Program[51] SORN	In accordance with the National Archives and Records Administration General Records Schedule for ethics program records, these records are generally retained for a period of six years after filing, or for such other period of time as is provided for in that schedule for certain specified types of ethics records. In cases where records are filed by, or with respect to, a nominee for an appointment requiring confirmation by the Senate when the nominee is not appointed and Presidential and Vice-Presidential candidates who are not elected, the records are generally destroyed one year after the date the individual ceased being under Senate consideration for appointment or is no longer a candidate for office. However, if any records are needed in an ongoing investigation, they will be retained until no longer needed in the investigation. Destruction is by shredding or electronic deletion.

[50] DHS/ALL-028 Department of Homeland Security Correspondence Records System (November 10, 2008), 73 FR 66657, *available at* https://www.gpo.gov/fdsys/pkg/FR-2008-11-10/html/E8-26691.htm.
[51] OGE/GOVT-1 Executive Branch Personnel Public Financial Disclosure Reports and Other Name-Retrieved Ethics Program (May 8, 2003), FR 24744, *available at* https://www.gpo.gov/fdsys/pkg/FR-2003-01-22/html/03-1101.htm.