Privacy Impact Assessment
for the

Office of the Chief Human Capital Officer

Workforce Analytics and Employee Records

DHS/ALL/PIA-075

September 27, 2019

Contact Point
Donna Seymour
Executive Director, Human Capital Business Solutions
Office of the Chief Human Capital Officer
Department of Homeland Security
(202) 357-8375

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

Abstract

Workforce Analytics and Employee Records is a Federal Human Capital Business Function whereby federal agencies implement a systematic process to review workforce and performance data, metrics, and results. Federal agencies conduct these reviews in an effort to anticipate and plan for future strategic and operational requirements and to make holistically informed Human Capital Management decisions. Specifically, federal human capital organizations generate evidence-based metrics to support decision-making concerning recruitment, staffing, training, and workforce development. The Workforce Analytics and Employee Records Business Function also facilitates compensation and benefits modeling, as well as the application of statistical models on such human resources (HR) issues as retention rates, time to on-board, retirement trends, and employee engagement. The Department of Homeland Security (DHS) is conducting this Privacy Impact Assessment (PIA) because the systems and data sources that support Workforce Analytics and Employee Records at DHS collect, use, store, and transmit personally identifiable information (PII) and sensitive personally identifiable information (SPII).

Overview

The DHS Office of the Chief Human Capital Officer (OCHCO) is responsible for conducting HR analyses and reporting for the Department. This includes advising the DHS Secretary on the selection, development, training, and management of a high-quality, productive workforce. It also covers evaluating human capital policies and programs to ensure compliance with federal laws and regulations and to promote human capital best practices. Accordingly, OCHCO frequently responds to recurring and ad hoc HR report requests[1] from internal and external customers such as DHS Component Human Capital Offices, the DHS Undersecretary for Management, the DHS Office of Inspector General, the U.S. Office of Personnel Management (OPM), the U.S. Government Accountability Office (GAO), Congress, the media, and private citizens making requests under the Freedom of Information Act (FOIA). OPM, the executive agency responsible for Federal Government-wide policy and guidance concerning human capital management, defines this type of HR analysis and reporting in its Human Capital Business Reference Model (HCBRM) as Workforce Analytics and Employee Records.[2]

[1] Recurring report requests are requests for a standard set of data provided to an authorized receiver on a regular reporting cycle. Ad hoc report requests are generally one-time requests for non-standardized singular or aggregated data.

[2] Human Capital Business Functions comprise the HCBRM, which is a model for federal agencies that defines the end-to-end lifecycle of Federal Government Human Capital Management (HCM). The model is used to streamline government-wide human resources operations, standardize HR service delivery, simplify HR acquisitions, and drive transparency in the federal budget. OPM categorizes Workforce Analytics and Employee Records in its Human Capital Business Reference Model as Function A9. For more information regarding OPM's HCBRM, and A9 specifically, *see* https://www.opm.gov/services-for-agencies/hr-line-of-business/hc-business-reference-model/hc-brm-interactive-model.pdf.

The majority of the tasks associated with Workforce Analytics and Employee Records are performed by OCHCO's Human Capital Data Analytics team (Data Analytics), which is part of OCHCO's Strategic, Workforce, Planning, and Analysis division. Data Analytics has four main objectives, all of which support the Workforce Analytics and Employee Records Business Function at DHS:

- Collect, inspect, clean, store, transform, and produce data so that customers can populate their reporting systems to complete day-to-day operations and processes;
- Produce analyses and data visualizations to stakeholders, including DHS senior leaders, DHS Components, Congress, the GAO, and the media;
- Develop and implement succession planning management across the Department to promote continuity of leadership and capabilities in critical skill areas; and
- Manage DHS response to annual OPM and U.S. General Services Administration (GSA) human capital performance metrics.

Data Sources

Data Analytics relies on several data sources to collect the information it processes into customer reports. Its primary data source is the Human Capital Enterprise Integration Environment (EIE), which is a secure data repository and segregated information-sharing environment that houses personnel data on every employee in the Department. Other data sources that supplement the information contained in EIE include the National Finance Center's (NFC) Insight system and NFC's Web Time and Attendance System (WebTA) system.[3]

EIE

EIE is a collection of hardware, software, and online data storage that supports the business and information needs of OCHCO. The system serves as a consolidated authoritative source for human capital information across the Department, and it functions as a data broker among all enterprise-level HR systems at DHS.[4] To support its information-sharing role, EIE houses a secure data repository containing personnel data on every employee at DHS. Most of the personnel data in the repository is populated via biweekly data feeds from NFC's Payroll/Personnel System (NFC PPS),[5] the official system of record for DHS civilian personnel.

[3] NFC is a federal agency under the U.S. Department of Agriculture's (USDA) Office of the Chief Financial Officer. It provides HR, financial, and administrative services for agencies across the Federal Government. For more information about NFC and its services, see https://www.nfc.usda.gov/.

[4] For example, EIE shares procurement-related personnel data with the Office of the Chef Procurement Officer's Enterprise Reporting Application (ERA) from across the Department to support DHS-wide procurement analysis and decision making. Another example involves EIE sharing personnel data with the Office of the Chief Information Officer's Management Cube (MGMT Cube). MGMT Cube aggregates the EIE data, along with data from other source systems, to enable the creation of analytic reports on DHS personnel, assets, financials, and budgeting.

[5] NFC PPS is an integrated payroll/personnel system offering a full range of personnel and payroll processing. It processes personnel actions; awards; allotments; bonds; performance appraisals; health and health insurance; thrift savings plan; tax documents; severance pay; leave records; and payroll-related financial reporting operations. For

Data Analytics manually extracts NFC source data from NFC PPS on a biweekly basis from files generated by the NFC PPS processing cycle. Source data manually downloaded by Data Analytics from NFC includes:

- A current snapshot of the full DHS Civilian Organizational Structure, containing NFC Organizational Codes, Agency Codes, Organizational Names, and Organizational Descriptions for levels within of the Department;
- A current snapshot of DHS Civilian Personnel information that includes information about the employee, the employee's organization, demographic information, and position information;
- Employee personnel action history, including nature of actions, effective dates of actions, and employee identification information;
- A list of all employees who have changed federal agency, occupational series, pay plan, and grade within the previous 18 months; and
- A list of all employees and their associated compensation leave time accrued, including hours earned, the associated pay periods, compensation already used since the beginning of the calendar year, and compensation time remaining.

Other sources of personnel data in EIE come from USA Staffing[6] and the Integrated Security Management System (ISMS).[7] The personnel information from USA Staffing pertains to new DHS job applicants, while the personnel information from ISMS pertains to the security status of new DHS hires.

EIE also collects person handles from ISMS. Person handle is a unique personal identifier that is assigned to every DHS employee and contractor at the time he or she passes his or her suitability determination to work at DHS. It was developed for use in lieu of Social Security number (SSN) to reduce privacy risks to DHS personnel. EIE generates a list of all employee and contractor SSNs that is sent to ISMS via a secure system connection. ISMS then associates a person handle to each SSN and returns this information to EIE via the same secure connection.

more information, *see* NFC PPS Payroll Personnel System (PPS) Redacted PIA, *available at* https://www.usda.gov/home/privacy-policy/privacy-impact-assessments.

[6] USA Staffing is an OPM shared service that guides federal agencies in the processing of new employees. For more information, *see* OPM's USA Staffing PIA, *available at* https://www.opm.gov/information-management/privacy-policy/privacy-policy/usas-pia.pdf.

[7] ISMS is a DHS-wide web-based case management application designed to support the lifecycle of the DHS personnel security, administrative security, and classified visit management programs. For more information, *see* DHS/ALL/PIA-038 Integrated Security Management System (ISMS), *available at* https://www.dhs.gov/privacy, and DHS/ALL-023 Personnel Security Management, 75 FR 8088 (February 23, 2010).

EIE is only available to the OCHO Human Capital Business Solutions (HCBS)[8] developers that support the system. They access the system using a username and password, after gaining access to the DHS network through single-sign on.

Insight[9]

Insight is a federal shared service[10] hosted by NFC that, like EIE, functions as a consolidated data warehouse with advanced reporting and business intelligence capabilities. Unlike EIE, however, the scope of the information housed in Insight covers every civilian employee in the Federal Government.

Insight provides NFC customers with workforce information that includes metrics and attributes to allow HR personnel to analyze staffing and productivity. The system is able to generate detailed employment reports, transactional processing reports, and case management reports reflecting information on any civilian employee in the Federal Government. The system can also generate management summary reports and dashboards containing drill-down analyses, trend analyses, and variance analyses.

Since EIE only collects a subset of the personnel information maintained by NFC concerning DHS employees, Data Analytics consults Insight whenever it receives a request that relies on personnel data not housed in EIE. Only certain employees within Data Analytics have Insight accounts, which they access using a username and password after gaining access to the DHS network through single-sign on. Any information collected from Insight is only used to satisfy Data Analytics report requests.

WebTA[11]

WebTA is a commercial-off-the-shelf (COTS) product designed exclusively for the Federal Government that tracks workforce attendance and leave. The system forwards the payroll records of every DHS employee to NFC at the end of each pay period for processing. The WebTA application is used by DHS employees to record hours worked, to request leave, and to obtain information regarding leave balances. Employees are required to enter their attendance information into the system and to validate that it is correct on a biweekly basis. The employee's

[8] OCHCO's HCBS division is responsible for managing all DHS-wide and OCHCO-specific HR Information Technology systems (HRIT). To this end, HCBS manages an IT service desk to support customers who need assistance with HRIT. When a request for IT support is initiated through the HCBS service desk, a ticket is created and tracked through HITS until the request is satisfied.

[9] For more information about Insight, a PIA is available on USDA's privacy policy website, https://www.usda.gov/home/privacy-policy/privacy-impact-assessments.

[10] A shared service is a business or mission function that is provided for consumption by multiple organizations within or between federal agencies. The goal of shared services is to efficiently aggregate resources and systems to improve the quality, timeliness, and cost effectiveness of service delivery to customers. For more information about federal shared services, *see* https://www.cio.gov/assets/files/sofit/02.04.shared.services.pdf.

[11] For more information about DHS's use of this system, please *see* DHS/ALL/PIA-009 DHS Web Time and Attendance (WebTA) System, *available at* https://www.dhs.gov/privacy.

supervisor also validates that the information is correct before it is sent to NFC for payroll processing.[12]

Data Analytics relies on WebTA for information requests related to employee time and attendance since this information is not housed in EIE or Insight. For example, if the DHS Secretary or the DHS Inspector General requests information related to how many hours a category of employees worked in any given pay period, Data Analytics would look to WebTA for this information. Similarly, if the DHS Secretary inquires how much labor expenses the Department is spending on a particular occupational series or geographic location, WebTA would serve as the appropriate data source for this information.

WebTA is accessed by DHS employees through federated single sign-on using Personal Identity Verification (PIV) cards,[13] Common Access Card (CAC) cards, or username/password and the time and attendance information they input into the system is transmitted to NFC on a biweekly basis via a secure communications link.

Reporting Tools

AXIS (also known as the Human Capital Reporting System (HCRS))

Information contained in EIE is displayed using an Oracle Business Intelligence application named AXIS.[14] AXIS is a multiple user, shared data reporting tool that uses role-based access to data within EIE to create reports, dashboards, and other Workforce Analytics and Employee Records work products. AXIS does not itself store data since its function is limited to retrieving, processing, and displaying information contained in EIE. AXIS is available to Data Analytics and the HCBS developers that support it. It is accessed using the federated single sign-on process.

Data Analytics uses AXIS to generate ad hoc and recurring reports by programming queries into the system and specifying how analysts want that information to display. AXIS then retrieves the queried information from EIE and displays it in the specified reporting format. These reports are saved and provided to the requestor using a means of transmission appropriate to their level of data sensitivity.[15]

Tableau

[12] A data refresh is performed every four weeks to re-synchronize the data in WebTA with the data at NFC.
[13] This process entails federal employees using their PIV cards to log into federal systems and networks. For a detailed explanation of PIV cards and their privacy implications, refer to DHS/ALL/PIA-014 Personal Identify Verification/Identity Management System (PIV/IDMS), *available at* https://www.dhs.gov/privacy.
[14] AXIS is not an acronym but is the actual name of the application.
[15] If the report contains PII or other sensitive information, it will be transmitted to internal DHS customers via Lockbox (see below) or by password-protected email. Transmission of sensitive reports to external DHS customers is accomplished via a secure portal managed by the customer, hand-delivered, or mailed in an opaque envelope via DHS courier.

Tableau is a COTS data visualization tool used by Data Analytics to create recurring reports in dashboard formats. Like AXIS, Tableau pulls data directly from EIE using a secure data connection; and Data Analytics uses information queries to specify the type of information to be retrieved from EIE, as well as the dashboard formats in which it is to be displayed. Report requestors may view the dashboards at their convenience by accessing Tableau using the federated single sign-on process.

Data Analytics only uses Tableau to satisfy recurring report requests when the requestor is an internal DHS customer. This ensures that everyone who accesses the tool and views the dashboards is subject to DHS's IT security controls. Moreover, Data Analytics only relies on Tableau to display reporting information that does not contain PII to minimize the risk that the information may be viewed by those without a need-to-know.[16]

The direct data connection from EIE to Tableau is managed by a database administrator who accesses EIE using a username and password, after gaining access to the DHS network through single-sign on. This database administrator is the only individual empowered to edit the connection or to view the information queries programmed into the tool by Data Analytics.

Reporting Procedures

Data Analytics retrieves the information it requires from the data sources listed above. When a customer requests a personnel or other HR-related report that requires the inclusion of PII, Data Analytics collects the necessary information from an appropriate data source, compiles the information, analyzes it, organizes it into an easily digestible report, and securely transmits the report either via a password-protected email or via Lockbox, an application of OCHO's HCBS[17] Information Ticketing System (HITS).

Lockbox

Lockbox is a SharePoint application[18] that enables secure report storage and delivery to customers internal to DHS. Data Analytics uses Lockbox to transmit all Workforce Analytics and Employee Records reports that contain PII to individuals and organizations within DHS. When a DHS Component first requests a report containing PII, Data Analytics creates a folder in Lockbox specifically for that Component. Subsequently, whenever a report is copied into a Component requestor's folder, the system automatically creates a copy of the report in a separate Lockbox

[16] Often, the information displayed on the dashboard relies on PII in EIE that has been aggregated in such a way that it cannot be tied back to individuals. In these cases, Data Analytics aggregates the PII in EIE before it is processed by Tableau into reports and dashboards to ensure the tool does not display PII.
[17] OCHCO's HCBS division is responsible for managing all DHS-wide and OCHCO-specific HR Information Technology systems (HRIT). To this end, HCBS manages an IT service desk to support customers who need assistance with HRIT.
[18] SharePoint is a web-based collaborative platform that integrates with Microsoft Office. It is primarily used as a document management and storage system, but the product is highly configurable and usage varies between organizations. For more information please *see* DHS/ALL/PIA-059 DHS Employee Collaboration Tools *available at* https://www.dhs.gov/privacy.

archive folder. This folder is accessible to Data Analytics and is primarily used for audit and recordkeeping purposes.

Data Analytics password-protects all reports sent via Lockbox and only provides the passwords to recipients and others with a verified need-to-know. These passwords carry over to the copies of the reports that are automatically moved to the archive folder.

Lockbox also contains a feature that enables automatic email notifications to requestors of ad hoc computer readable extracts (CRE) that remind them to delete the information they receive after 90 days.[19]

HITS

Lockbox is an application of HITS, which is an OCHCO-managed SharePoint application that is used by OCHCO customers to initiate a request for IT service or support through the HCBS service desk. The types of IT service requests received in HITS are various, and include HRIT system enhancements, assistance addressing system errors, new user account requests for HRIT, and system training requests. HITS is also frequently used to request HR reports, and such requests are forwarded to Data Analytics for execution. When Data Analytics receives a report request, it creates a service ticket in HITS, and then it uses the ticket as a means of tracking implementation until the request is fulfilled.

HITS collects user names and email addresses for the purpose of authenticating users once they are added to the appropriate role categories in SharePoint. This is the only PII ingested into the system other than the rare customer report containing PII that is transmitted to internal customers via Lockbox.

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?

5 U.S.C. § 1401[20] – requires the head of a government agency to appoint or designate a Chief Human Capital Officer, who shall (1) advise and assist the head of the agency and other agency officials in carrying out the agency's responsibilities for selecting, developing, training,

[19] DHS 4300A Sensitive Systems Handbook, Appendix S1 defines CRE as "any federal record or collection of records containing sensitive PII that is retrieved from a DHS-owned databased, through a query, reporting tool, extract generation tool, or other means that is then saved into removable media and/or a separate computer-readable device or application such as another database, a spreadsheet, or a text file." Section 1.2 of this guidance requires that all CREs "be erased within 90 days unless the information included in the extracts is required beyond the 90-day period." This same section requires the owner of the data to document the permanent erasure of CREs or the need for continued use every 90 days; and it requires the Component Privacy Officer to periodically audit compliance with this requirement. OCHCO audits Lockbox biannually to ensure compliance with these requirements.

[20] Chief Human Capital Officers Act of 2002 - enacted as part of the Homeland Security Act of 2002 (Pub. L. No. 107-296) on November 25, 2002.

and managing a high-quality, productive workforce in accordance with merit system principles; (2) implement the rules and regulations of the President and OPM and the laws governing the civil service within each agency; and (3) carry out such functions as the primary duty of the Chief Human Capital Officer.

5 U.S.C. § 1402 – requires Chief Human Capital Officers to assess and measure the workforce of the agencies they serve.

5 U.S.C. § 2951 – requires an agency to inform OPM about employees' employment status.

44 U.S.C. § 3101 – requires that federal agencies make and preserve records containing documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency.

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

Information collected, maintained, used, and disseminated by DHS and OPM on employees in support of Workforce Analytics and Employee Records is covered by the following SORNs:

- OPM/GOVT-1 General Personnel Records, 77 FR 73694, December 11, 2012;
- OPM/GOVT-2 Employee Performance File System Records, 71 FR 35347, June 19, 2006;
- DHS/ALL-003 Department of Homeland Security General Training Records, 73 FR 71656, November 25, 2008;
- DHS/ALL-019 Department of Homeland Security Payroll, Personnel, and Time and Attendance Records, 73 FR 63172, October 23, 2008; and
- DHS/ALL-023 Personnel Security Management, 75 FR 8088, February 23, 2010.

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

Yes. EIE and AXIS are minor applications of the CHCO Virtual Production Enclave (VPE) and are therefore covered by the CHCO VPE system security plan, which was completed on May 14, 2019. CHCO VPE has entered Ongoing Authorization and its current Authority to Operate expires April 21, 2020.

Tableau is covered by the DHS Business Intelligence as a Service system security plan, which was completed on November 14, 2018. Its current Authority to Operate expires November 19, 2020.

HITS and Lockbox are SharePoint applications and are therefore covered by the DHS SharePoint as a Service system security plan, which was completed on October 9, 2018. Its current Authority to Operate expires August 23, 2020.

The system security plans for NFC Insight and NFC WebTA were developed and are managed by NFC. The system security plan completion dates and Authority to Operate expiration dates for these two systems may be obtained directly from that agency.

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

The NARA General Records Schedule (GRS) 2.0 Human Resources series and 5.0 General Operations Support series cover all of the categories of information contained in EIE and the other systems that support Workforce Analytics and Employee Records at DHS.[21] Specifically, the following General Records Schedules apply:

- Individual Employee Records: GRS 2.2, item 041 (DAA-GRS-2017-0070005);
- Records Used to Calculate Payroll: GRS 2.4, item 010 (DAA-GRS-2016-0015-0001);
- Time and Attendance Records: GRS 2.4, item 030 (DAA-GRS-2016-0015-0003);
- Non-mission Employee Training Records: GRS 2.6, item 010 (DAA-GRS-2016-0014-0001);
- Individual Employee Training Records: GRS 2.6, item 030 (DAA-GRS-2016-0014-0003);
- Administrative Records Maintained in any Agency Office: GRS 5.1, item 010 (DAA-GRS-2016-0016-0001); and
- Security Administrative Records: GRS 5.6, item 010 (DAA-GRS-2017-0006-0001.

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.

Workforce Analytics and Employee Records information is not covered by the PRA because information is collected from DHS employees and contractors and not from the general public.

[21] Specific retention rules for these two GRS series are available at https://www.archives.gov/records-mgmt/grs.html.

Section 2.0 Characterization of the Information

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

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

EIE serves as DHS's authoritative data source for all information processed as part of DHS's Workforce Analytics and Employee Records Human Capital Business Function.[22] EIE collects and maintains personnel and organizational data necessary to provide enterprise-wide human capital reporting to DHS customers. DHS customers primarily use this data to populate their own reporting systems and to complete day-to-day HR processes and operations. Direct dissemination of personnel data from EIE to DHS customers includes SPII that is relayed directly via a secure data connection to other DHS systems.

At customers' requests, SPII and other information in EIE is processed into recurring and ad hoc reports that are aggregated in such a way as to no longer be linkable to individuals. These Data Analytics reports are usually transferred through Lockbox or made available to customers on Tableau. Customers of Workforce Analytics reports vary, and include DHS Component Human Capital Offices, the DHS Undersecretary for Management, the DHS Office of the Inspector General, OPM, GAO, Congress, the media, and private citizens making FOIA requests.

EIE collects the following data from other source systems on a biweekly basis:

- Data sets from NFC PPS pertaining to personnel information of DHS employees, personnel action history, personnel payroll, pay period information, relocation of employees among DHS Components, available employee attendance and leave, organizational structure, and sick, annual, and other leave taken;
- Data sets from USA Staffing pertaining to personnel information for new DHS job applicants;
- Data sets from ISMS pertaining to personnel information for new hires, including person handle;
- A data set from the U.S. Coast Guard pertaining to its military personnel.

EIE transmits the following data on a regular basis via a secure connection to other DHS systems:

- Data sets to DHS's Management Cube[23] for aggregation by that system into business intelligence reports. The data sets pertain to personnel and employment

[22] All of the information processed through other DHS systems that support Workforce Analytics and Employee Records at DHS rely on data from EIE or from systems managed by NFC. While these other DHS systems display data contained in EIE and NFC systems in various reporting formats, they do not themselves store information.
[23] DHS's Management Cube is a business intelligence tool that houses financial, acquisition, human resources, contracting, asset, and security data about DHS and its personnel for executive management analysis and decision-

information, employee job position, organizational structure, employee payroll, personnel data structure, current pay period, employee pay plan, veterans status, and disability status.

- Data sets to the Performance and Learning Management System (PALMS)[24] for employee learning and development needs. The data sets pertain to personnel and employment information for DHS employees, personnel and employment information for non-DHS employees who take DHS-sponsored training,[25] employee organization, job title, and user email.
- Data sets to DHS's Active Directory. The data sets pertain to personnel time and attendance, organizational structure, and personnel information of employees recently separated from DHS.
- Data sets to the U.S. Citizenship and Immigration Services (USCIS) Human Capital Office to help it manage HR functions for its employees. The data sets pertain to employee and personnel information of USCIS employees, personnel action history of USCIS employees, and USCIS organizational structure.
- Data sets to the DHS Office of the Chief Security Officer (OCSO) to help it manage processes related to the physical security of the Department and its personnel. The data sets pertain to employees recently separated from DHS and employee email contact information.
- A data set to ISMS pertaining to personnel information for new DHS job applicants.[26]
- Data sets to the U.S. Customs and Border Protection (CBP) pertaining to CBP employee identification information.
- Data sets to the DHS Office of the Chief Procurement Officer (OCPO) pertaining to employees across DHS in the contracting federal job series.

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

The sources of information for Workforce Analytics and Employee Records are those systems described in Section 2.1 from which EIE collects data on a biweekly basis, as well as NFC Insight and NFC's WebTA. Specifically, the source systems for EIE include NFC PPS, USA

making. For more information, *see* the forthcoming Management Cube PIA, which will be *available at* https://www.dhs.gov/privacy.

[24] DHS's PALMS is a consolidated learning management system that supports workforce training. For more information, *see* DHS/ALL/PIA-049 Performance and Learning Management System (PALMS), *available at* https://www.dhs.gov/privacy.

[25] Employees from other federal agencies may take DHS-sponsored training. On these rare occasions, basic training records are created for them in PALMS that consist of name, agency, work contract information, and ultimately whether they successfully complete the course. These records are transferred into EIE along with the more extensive training records maintained for DHS employees.

[26] These are the same 100 data elements that are collected biweekly from USA Staffing.

Staffing, and ISMS. All information from these source systems is transmitted to EIE via a secure data connection that is administered by a single EIE administrator.

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. All of the data stored in EIE or processed through other Workforce Analytics tools at DHS consist of personnel and organizational information regarding DHS employees and contractors.

2.4 Discuss how accuracy of the data is ensured.

Each EIE data source owner conducts its own data accuracy assessments prior to EIE ingesting its data. During the data ingestion process, EIE conducts automated business logic validation tests and rejects records that do not pass. Data that does pass validation is then ingested into the system without alteration. EIE also employs tagging mechanisms and automated quality controls that identify inconsistences among similar data sets to ensure data integrity and quality.

2.5 Privacy Impact Analysis: Related to Characterization of the Information.

Privacy Risk: There is a risk that EIE users may be able to access information about individuals in the system they do not need in the performance of their duties.

Mitigation: This risk is partially mitigated. EIE contains specific security controls that require database accounts. These accounts are granted on a need-to-know basis only. Prior to gaining access to EIE, approvals must be obtained from the system owner and the Information System Security Officer (ISSO). EIE relies on the DHS Data Center to manage the servers that support EIE, which are maintained in accordance with security practices outlined in DHS 4300A, *Sensitive Systems Handbook*.[27] Access to EIE is also role-based, meaning that certain PII is hidden from view for certain users who do not have a need-to-know that specific information.

Privacy Risk: There is a risk that EIE will collect more information about individuals than is needed for the type of analysis and decision-making the system is designed to support.

Mitigation: This risk is partially mitigated. The data elements regarding information about individuals extracted from source systems are a subset of what is collected by those systems and are based on the specific needs of DHS. However, the information collected is not specifically tailored to any particular type of data request because it is difficult to predict what type of Workforce Analytics report requests will be needed by customers.

[27] DHS 4300A Sensitive Systems Handbook, *available at* https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook.

Privacy Risk: There is a risk that EIE data analysts will combine data elements from more than one source system to create a more sensitive data set than each individual source system would be able to generate alone.

Mitigation: This risk cannot be fully mitigated. However, data in EIE are logically segregated by source system into separate database schemas. This allows EIE to implement strict access controls over all data. Users are only granted access to schemas to which they have a verified need-to-know.

Privacy Risk: There is a risk that EIE contains inaccurate data due to the latency of data transfers.

Mitigation: This risk is partially mitigated. Data in EIE is updated programmatically as quickly as possible, often within 24 hours, and in some cases within minutes of the data being updated in the source system. The data sets that take longer to update require manual intervention. These data sets, however, are updated every other week in the source system, further mitigating the risk of outdated data in EIE.

Section 3.0 Uses of the Information

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

3.1 Describe how and why the project uses the information.

Data Analytics uses the information in EIE, NFC Insight, and WebTA to analyze issues and generate reports that executives and analysts can rely on to make HR and other management decisions. These reports are typically aggregated such that the information they contain is not linkable to individuals. When responding to report requests, Data Analytics does not collect information directly from individuals, but rather aggregates data from Workforce Analytics and Employee Records source systems to create management reports pertaining to the DHS workforce. Such reports typically rely on aggregated demographic data, calculations of retirement eligibility, and other macro-level data analyses. These reports are typically generated in response to requests by DHS customers seeking information to support executive decision-making.

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.

Data Analytics frequently conducts electronic searches using AXIS to identify predictive patterns or anomalies. However, Data Analytics does not link this information back to individuals. For example, a Workforce Analytics and Employee Records customer might request a report from Data Analytics showing a trend line illustrating the use of a certain leave category across a particular DHS Component. While the trend line will communicate at a high level how much of

that leave is being taken by personnel across the organization and may be taken in the future, it does not speak to any particular individual's use of leave.

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

Only OCHCO employees may access EIE. Some employees in Component Human Capital Offices are granted access to AXIS, but they can only query information relevant to employees within their particular Component.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk associated with individuals gaining unauthorized access to information in EIE or reporting capabilities in AXIS.

Mitigation: This risk is mitigated. Information security and policy controls for EIE and AXIS are inherited from CHCO VPE because they are considered minor applications of CHCO VPE. All CHCO VPE IT security and policy controls comply with DHS *4300A, Sensitive System Handbook*. Specific controls include requiring database accounts to access the system only on a need-to-know basis and subject to the approval of the system owner and the ISSO. Password resets are also required at least every 90 days and accounts are disabled upon expiration. AXIS is also accessed using the federated single-sign on process, which means system level and database level access is only available on the DHS network and via use of the employee's PIV card.

Privacy Risk: There is a risk that incorrect information in employee records contained in EIE or displayed in AXIS could lead to faulty or unjust personnel decisions.

Mitigation: This risk is partially mitigated. EIE functions as a data repository and broker between other systems. AXIS is a business intelligence tool used to generate analytical reports and trend analyses to support executive decision-making. Neither of these systems is in any way used to review individual employee data or to process personnel actions or decisions. Rather, monitoring and management of data about individual employees, and processing of personnel decisions, are conducted using source systems of EIE such as NFC PPS, WebTA, FedHR Navigator,[28] Electronic Official Personnel Folder (OPF),[29] and USA Staffing.

[28] FedHR Navigator is a COTS system that automates federal HR functions and assists the strategic management of human capital within the federal workforce. It is used by agencies throughout the Federal Government and consists of a suite of web-based software tools accessible by employee and HR personnel. More information about FedHR Navigator may be found on the FedHR Navigator vendor's website, *located at* https://www.econsys.com/fedhr-navigator/.

[29] A federal employee's Official Personnel Folder (OPF) contains all the official records required to document his or her career. Documents referenced as those on the "left side" are considered temporary and therefore change as a federal employee's career progresses. Consequently, they are not kept for the life of the folder and are subject to records disposition dates. Documents on the "right side" of the file are long term and are therefore kept for the life of the OPF (*i.e.*, they follow employees throughout their careers and are only dispositioned after the employee leaves federal service). The Electronic OPF (eOPF) is an electronic version of the OPF used by the vast majority of

Section 4.0 Notice

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

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

Systems supporting Workforce Analytics and Employee Records at DHS do not collect information directly from individuals. Rather, the information comes from NFC or DHS source systems that themselves may collect directly from individuals. Individuals providing information that is transmitted to NFC PPS, NFC Insight, and EIE, are provided notice at the time of initial collection by Privacy Act Statements informing the individuals of the authority for and purpose of the collection, the uses of the information, and whether providing the information is mandatory. Notice is also provided by this PIA and PIAs related to those systems, as well as the publication of the SORNs identified in Section 1.2.

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

NFC PPS, Insight, and other EIE source systems provide individuals with notice and an opportunity to provide consent to the stated uses of their information (*e.g.*, personnel data collections prior to beginning work as an employee or contractor). Although individuals do not have a separate opportunity to consent to the use of their data in EIE, they may seek correction of their data if needed. OCHCO relies on EIE to support a vast majority of the mandatory processes that support employment at DHS, and thus it would not be feasible to continue to employ an individual who opts out of having their information stored in EIE.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals providing personnel-related data about themselves to OCHCO do not have notice that some of their personal information will be maintained in EIE.

Mitigation: This risk is partially mitigated by publication of this PIA, and through the SORNs referenced in Section 1.2. Although there is no specific notice of the use of information in EIE at the point of collection by NFC, DHS personnel may reasonably expect that personal information may be used for administrative and managerial functions at their agencies of employment.

federal agencies and a system managed by OPM for accessing the electronic folder online. For more information regarding eOPF and its privacy implications, *see* OPM's eOPF PIA, *available at* https://www.opm.gov/information-management/privacy-policy/privacy-policy/eopf-pia.pdf.

Section 5.0 Data Retention by the project

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

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

OCHCO worked with the DHS Records Management Office to develop a data retention policy for EIE that specifies a three-year retention period for each major category of information contained in the system. The following table summarizes the categories of information in EIE, the controlling records schedules for each, and the justifications for setting a three-year retention period.

	Description	**Disposition**	**Retention**	**Justification**
Individual Employee Records **GRS 2.2, item 041 (DAA-GRS-2017-00070005)**	Records of separated employees saved to the "temporary" folder in the eOPF or filed on the left side of the hardcopy OPF, or their equivalent.	Destroy when superseded or obsolete, or upon separation or transfer of employee.	3 years	OCHCO does not consider these records obsolete until three after an employee separates to support its business need to generate management reports and trend analyses that aggregate workforce data from previous years. These deliverables are provided to senior DHS leaders and decision makers who need to make management decisions about the DHS workforce and who need to respond to DHS oversight bodies. This three-year retention period also allows OCHCO to effectively respond to FOIA requests for

				information about employees who separated from the Department within recent years.
Payroll Records **GRS 2.4, item 010 (DAA-GRS-2016-0015-0001)**	Records used to calculate payroll, arrange paycheck deposit, and change previously issued paychecks.	Destroy 2 years after employee separation or retirement, but longer retention is authorized for business use.	3 years	OCHCO has a business need to retain these records for three years after an employee separates, in support of its business need to generate management reports and trend analyses that aggregate workforce expenditure data from previous years. These deliverables are provided to senior DHS leaders and decision makers who need to make management decisions about workforce cost planning and who need to respond to DHS oversight bodies.
Time and Attendance Records **GRS 2.4, item 030 (DAA-GRS2016-0015-0003)**	Sign-in/sign-out records, time cards, leave applications and approvals of all types (annual, sick, family medical, military service,	Destroy after GAO audit or when 3 years old, whichever is sooner.	3 years	OCHCO retains these records for 3 years in accordance with the governing GRS.

	jury duty, leave donations, etc.); overtime, compensatory, and credit time requests and approvals; premium pay authorizations; and other records documenting employees' presence at or absence from work.			
Non-mission Training Records **GRS 2.6, item 010 (DAA-GRS-2016-0014-0001)**	Records about planning, assessing, managing, and evaluating an agency's training program.	Destroy when 3 years old, or 3 years after superseded or obsolete, whichever is appropriate, but longer retention is authorized if required for business use.	3 years	OCHCO retains these records for 3 years in accordance with the governing GRS.
Individual Employee Training Records **GRS 2.6, item 030 (DAA-GRS-2016-0014-0003)**	Records documenting training required by all or most federal agencies, such as information system security and anti-harassment training, and	Destroy when superseded, 3 years old, or 1 year after separation, whichever comes first, but longer retention is authorized if	3 years	OCHCO has a business need to retain these records for three years after an employee separates in support of its business need to generate management reports that aggregate employee training data from previous

	training to develop job skills.	required for business use.		years. These deliverables are provided to senior DHS leaders and decision makers who need to make management decisions about future course offerings and training opportunities and who need to respond to DHS oversight bodies.
Administrative Records **GRS 5.1, item 010 (DAA-GRS-2016-0016-0001)**	Records accumulated by individual offices that relate to routine day-to-day administration and management of the office rather than the mission-specific activities for which the office exists, including staff locators, unofficial organizational charts, and office seating charts.	Destroy when business use ceases.	3 years	OCHCO has a business need to retain unofficial organizational charts in EIE for three years after the records become obsolete to support its business need to generate management reports that document and evaluate prior organizational structures. These deliverables are provided to senior DHS leaders and decision makers who need to engage in organizational planning and who need to respond to DHS oversight bodies.

Security Administrative Records **GRS 5.6, item 010 (DAA-GRS-2017-0006-0001)**	Records about routine facility security, protective services, and personnel security program administration. Includes status reports on cleared individuals and other reports.	Destroy when 3 years old, but longer retention is authorized if required for business use.	3 years	OCHCO retains this information for 3 years in accordance with the governing GRS.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that the information in EIE will be retained on an individual longer than is necessary to accomplish a legitimate purpose, or inconsistently with the records retention schedule.

Mitigation: This risk is mitigated. OCHCO's data retention policy is to retain information about employees for three years after separation from DHS. This retention period was developed in coordination with the DHS Records Management Office and complies with the GRS listed above. On a quarterly basis, the HCBS team conducts an audit to find all personnel files in EIE that have not received a payroll record within the past three years. Any employee that shows as not having been paid within the past three years will have all records associated to them removed.

Section 6.0 Information Sharing

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

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

Workforce Analytics reports are sometimes provided to external DHS customers and stakeholders to satisfy congressional inquiries, inquiries from other federal agencies, and FOIA requests. Information transmitted to Congress and other federal agencies is aggregated in such a way as to make it impossible to link it back to individuals. In the rare case that PII is requested in a report by an external customer or stakeholder, CHCO will communicate that request to the Component whose data is involved before sharing that data to the requester. In the case of FOIA requests, disclosure is either required by law or relates to the individual making the request.

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

The SORNs applicable to Workforce Analytics and Employee Records permit the sharing of personnel and organizational records with external entities to support certain human resources and management functions. The routine uses in the SORNs define the circumstances for when information may be shared externally. A complete list of the routine uses can be found in the listed SORNs. The following are examples of information sharing permitted by routine uses:

- Information may be shared with contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. (*Routine Use JJ*, OPM/GOVT-1 General Personnel Records).
- Information may be shared with other federal agencies who provide payroll personnel processing services under a cross-servicing agreement for purposes relating to the conversion of DHS employee payroll and personnel processing services; the issuance of paychecks to employees and distribution of wages, and the distribution of allotments and deductions to financial and other institutions, some through electronic funds transfer (*Routine Use K,* DHS/ALL-019 Payroll, Personnel and Time and Attendance Records System of Records).

6.3 Does the project place limitations on re-dissemination?

Yes, OCHCO's Privacy Standard Operating Procedures (SOP) require that the Executive Director of HCBS "approves requests for Computer Readable Extracts (CRE), confirming that the creation and disclosure of the CRE is consistent with DHS 4300A Attachment S1, Managing CREs Containing SPII."[30] The SOP also requires OCHCO program managers to forward requests for ad hoc CREs to the HCBS Executive Director for review and approval; to use Lockbox for disseminating, tracking, and verifying CREs and other large files for internal distribution; to seek reauthorization of CRE requests after 90 days when the information included in the extracts is required beyond the 90 day period; and to confirm ad hoc CREs are destroyed when no longer needed and not later than 90 days after the creation date unless the HCBS Executive Director has reauthorized beyond 90 days.

6.4 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that individuals authorized to access EIE and AXIS will conduct unauthorized activities such as extracting and sharing information with unauthorized recipients.

[30] *Available at* https://www.dhs.gov/sites/default/files/publications/4300A-Handbook-Attachment-S1-Managing-CREs-Containing-SPII.pdf.

Mitigation: This risk is partially mitigated. Although there are no physical barriers preventing system administrators from extracting information from EIE and sharing it with unauthorized recipients, they are required to sign a *Rules of Behavior* document prohibiting such practices. Additionally, all user accounts require approval from the system owner and the ISSO. EIE and AXIS also contain audit history logs. The EIE audit history log details who accessed the system and when. The audit history log for AXIS details what information was accessed, which users accessed it, and when it was queried from the system.

Section 7.0 Redress

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

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

Employee records collected, maintained, used, and disseminated by DHS are covered by the Privacy Act. Employees may file a Privacy Act or FOIA request with DHS or OPM to access their personnel records. In addition, employees may access personnel data about themselves via NFC's Employee Self Service page (MyEPP).[31]

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

If an employee knows of any inaccurate or erroneous information about him or herself in any of these systems, the employee may contact the appropriate HR specialist within his or her human resources servicing unit who will liaise with the appropriate IT personnel at the source system agency to correct the information. The employee may also submit an HR ticket through FedHR Navigator to request correction of inaccurate or erroneous information about him or herself.

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

Each DHS organization has one or more designated HR specialists to assist with HR needs. The names and titles of these individuals are common knowledge throughout organizations and are reflected on organization charts. Employees may also reach out to OCHCO or any of the Component Human Capital Offices using the general HR phone numbers and email addresses posted on the DHS employee intranet site. Additionally, they may submit an HR service ticket through FedHR Navigator to correct inaccurate information, or they may correct some of their

[31] *See* https://www.nfc.usda.gov/EPPS.

personal information themselves via NFC's Employee Service page (MyEPP). Links to FedHR Navigator and MyEPP are prominently displayed on the DHS employee intranet homepage.

7.4 Privacy Impact Analysis: Related to Redress

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

Mitigation: This risk is mitigated. Employees routinely use MyEPP to update and correct their personnel data. Employees also have HR representatives assigned to them who can assist with all types of HR matters. Additionally, all government personnel records are covered by the Privacy Act, and fall under the general personnel records SORNs managed and maintained by DHS and OPM. There are Privacy Act notices on all OPM and DHS IT systems that alert candidates and new employees that their records are afforded Privacy Act protections.

Section 8.0 Auditing and Accountability

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

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

Workforce Analytics and Employee Records reports that contain SPII are logged using the Lockbox application. Per OCHCO's Privacy SOP, the HCBS Executive Director is responsible for ensuring Lockbox is audited at least biannually to validate that all reports containing PII are purged within 90 days of transmission, unless the Component has attested to the need to retain it beyond 90 days per the CRE requirements defined in DHS 4300A Sensitive Systems Handbook, Appendix S1. Additionally, ad hoc reports transmitted via Lockbox are password-protected and stored in restricted folders accessible only by the requestor of the report. Furthermore, Data Analytics reviews requests for reports and determines whether the requestor is authorized to receive the data, whether it is feasible to address the request, and whether the work product requested is consistent with Routine Uses specified in the applicable SORN.

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

OCHCO Data Analytics personnel, as well as all OCHCO personnel, complete Privacy and IT Security Awareness Training at least annually. System, database, and application administrators also must complete privileged user training, system administrator training, and incident response training prior to assuming those roles.

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

Access to DHS systems that support Workforce Analytics and Employee Records rely on a documented and formal process overseen by HCBS IT security personnel. The program managers for these systems determine who may access them and the roles to be granted. HCBS IT security personnel work with the user and endorser to complete paperwork and to ensure compliance with mandatory training requirements. This procedure is documented in the system security plans referenced in Section 1.3. At a minimum, access to DHS systems that support Workforce Analytics and Employee Records are role-based and based on a need-to-know.

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?

All changes to EIE, whether they relate to data elements, system interchanges, security features, or other features that affect the information or architecture of EIE, must be approved by the EIE system owner, by an HCBS ISSO, and by an HCBS privacy analyst prior to deployment. This is accomplished using an automated ticketing system that streamlines the review and approval process. New information sharing agreements, Memoranda of Understanding (MOU), and new access by external organizations to DHS tools and applications supporting Workforce Analytics and Employee Records are approved in advance by the HCBS Executive Director and by the DHS Privacy Office.

Responsible Officials

Donna Seymour
Executive Director
Human Capital Business Solutions
Office of the Chief Human Capital Officer
Department of Homeland Security

Approval Signature

Original, signed copy on file with the DHS Privacy Office.

_____

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