Version Number: 01-2017

U.S. Department of Commerce
Office of the Secretary

Privacy Impact Assessment
for the
Office of Human Resources Management (OHRM) OHRM Apps

Reviewed by: Kathleen Gioffre, Office of the Secretary (OS) Privacy Officer

☑ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

For Dr. Catrina D. Purvis LISA MARTIN Digitally signed by LISA MARTIN
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=LISA MARTIN, 0.9.2342.19200300.100.1.1=13001000105292
Date: 2018.05.18 07:55:01 -04'00'

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
Office of the Secretary
Office of Human Resources Management (OHRM) OHRM Apps

Unique Project Identifier: OS-059 Enterprise Application System OS-008 OHRM General Support System

Introduction: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

(a) Whether it is a general support system, major application, or other type of system

The OHRM is responsible for planning, developing, administering and evaluating the human resources management programs of the Department. This enables the Department to acquire and manage a dedicated, diverse, motivated, and highly qualified workforce to accomplish its mission and achieve its goals, while ensuring compliance with pertinent Federal, Office of Personnel Management, Office of Management and Budget, and Department of Labor, policy and administrative mandates.

(b) System location

The systems are primarily managed by resources located at the CBS Solutions Center in Gaithersburg, MD. The system is physically located at the Federal Aviation Administration Data Center (DOT/FAA/ESC) in Oklahoma City, OK.

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

For the purpose of payroll and payment processing, Human Resources (HR) personnel data files from OHRM's Pay for Performance System (PPS) and SES Bonus Pool System (SES BP), are batched to USDA's NFC database. A second file is uploaded to Department of Treasury's HR Connect System for future department wide all-in-one front-end HR system.

Data from CLC Datafeed is uploaded to the LMS vendor Cornerstone On Demand, as a part of their user integration application.

The system also obtains data from USDA for PPS, CLC Datafeed, and the SES Bonus Pool.

(d) The way the system operates to achieve the purpose(s) identified in Section 4

The OHRM utilizes a wide variety of HRIT systems to provide Department-wide human resources services. The GSS system performs vital Human Resource (HR) functions to support OHRM business.

- Automated Classification System (ACS) – ACS contains key position data that supervisors use to create and simultaneously classify project position descriptions. In addition to creating new position descriptions, the ACS stores descriptions in a local user database and allows the user to create a new description based on one in the database; to revise, review, print, or delete descriptions; or to review and report on the descriptions in the database.
- Performance Payout System (PPS) – PPS provides the functionality to record, document and report the annual employee performance rating, performance increase, bonus payout and calculate the annual comparability increase (ACI) for the employees who are under the Commerce Alternative Personnel System (CAPS) pay plans and transmit updated data to the U.S. Department of Agriculture's National Finance Center (NFC) – the Department's Payroll System of Record.
- ERIS- End of Year – Senior Executive Service (SES) Bonus Pool (BP) – SES BP provides the functionality to record and report the annual performance ratings, performance increases, and bonus recommendations, and calculate the annual comparability increases (ACIs) for the SES employees and transmit the updated data to NFC.
- Executive Resources Information System-Top Level (ERIS-TL) – provides information regarding the incumbency status of all key positions to aid in Executive Level (SES) Staffing decisions.
- DOC-Hiring Management System (DOC-HMS) – HMS tracks and reports on the timeliness of the hiring process, and hiring actions initiated by the DOC's Human Resources Operations Center (DOCHROC) as part of the overall human resources management measurement project. This system tracks all the hiring steps from the job announcement to the day the new employee reports for duty. It tracks each step of the process and produces the necessary reports to measure the process effectiveness and efficiency. Reports are generated as part of the DOCHROC metrics for management purposes.
- Honor Award Nominee System (HANS) – HANS is an automated Gold and Silver Honor Awards Program nomination and reporting system. This system provides users' access to nominate employees and vote on nominations, and produce reports including certificate citations, program booklets, and seating charts.
- CLC Datafeed Database - CLC Datafeed is an outbound feed containing department-wide employee and non-employee personnel data used for account creation and maintenance for the Learning Management System (LMS).

(e) How information in the system is retrieved by the user

Users can only print reports pertaining to their assigned roles within all of the HR Systems. Their local printers or high-speed printers in their office vicinity. It is the responsibility of the users to handle printed media in accordance with established policies/procedures/rules of behavior and governmental record retention regulations of their bureau and DoC. Users can download information, again based on their assigned user role within the HR Systems , to removable media and it is their responsibility to handle digital media in accordance with established policies/procedures/rules of behavior and governmental record retention regulations of their bureau and DOC.

(f) How information is transmitted to and from the system

Information is transmitted across approved encryption protocols such as HTTPS, SSH, and SFTP. Sensitive data transmissions are encrypted according to NIST 800-18, Federal Information Processing Standards (FIPS) 186, Digital Signature Standard and FIPS 180-1, and Secure Hash Standard issued by NIST when necessary.

(g) Any information sharing conducted by the system

All access to the HR Systems are unique userids and passwords given by the application Administrator or CSC resource. Each user is assigned permission levels depending on the functional role they perform within the HR applications and these roles are tied to their userids. Users must request access and get approval from their supervisor's and Bureau POC, or CSC resource before obtaining access to the HR applications.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

Includes the following, with all revisions and amendments: 5 U.S.C. 301; 44 U.S.C. 3101; Executive Office (E.O.) 12107, E.O. 131614, 41U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999, DAO 202-430 (performance management system), DAO 205-16 management of electronic records.

The authority to deliver, maintain, and approve Department-wide and bureau-specific automated human resources systems and serve as the focal point for the collection and reporting of human resources information within the Department of Commerce (DOC) is delegated to the Office of Human Resources Management (OHRM). This authority is identified by Departmental Organization Order (DOO) -- 20-8 - SECTION 4.

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

The OHRM Applications are part of the Enterprise Applications Systems (EAS) OS-059, which is categorized as MODERATE.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

_____ This is a new information system.
_____ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System		f. Commercial Sources		i. Alteration in Character	

Management Changes				of Data	
j. Other changes that create new privacy risks (specify):					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

_X__ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*	X	e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID	X	g. Passport		k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: SSN usage is minimized. However, it is used to ensure accurate employee reporting, and is a required unique identifier for NFC.					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth	X	m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	X
c. Alias		i. Home Address	X	o. Medical Information	
d. Gender	X	j. Telephone Number	X	p. Military Service	
e. Age	X	k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity	X	l. Education	X	r. Mother's Maiden Name	
s. Other general personal data (specify): Gender, Age, Race/Ethnicity, & Education are only used by the CLC database for metrics and reporting.					

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	X
b. Job Title	X	e. Email Address	X	h. Work History	X
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify): Salary, bonus, pay increase information, series, grade, and Entrance on Duty (EOD) date.					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address	X	d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax	X	Online	X
Telephone	X	Email			
Other (specify): Secure file transfer - Accellion					

Government Sources					
Within the Bureau	X	Other DOC Bureaus	X	Other Federal Agencies	X
State, Local, Tribal		Foreign			
Other (specify):					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Describe how the accuracy of the information in the system is ensured.

For PPS, SES Bonus Pool, and the CLC Datafeed information is directly imported from DOC's primary data source, NFC. Information is not altered by CSC staff. Top Level, HMS, HANS and ACS, information is directly inputted by the authorized users of the system and not CSC resources. Audit logs confirm input into the systems.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act.

	Provide the OMB control number and the agency number for the collection.
X	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

X	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	X
For administrative matters	X	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online	X	For employee or customer satisfaction	

For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): For metrics & report generation. Information from NFC dictates pay related eligibility used in Bonus Pool and PPS.			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

- ACS contains key position description data about departmental pay band (CAPS) positions that supervisors use to create and simultaneously classify Demonstration Project position descriptions.
- PPS information collected is intended to ensure accurate rating and ranking of CAPS employees' performance and based on the performance rating, calculate salary increase and bonus payout. Payroll Data from NFC's database is used to help determine eligibility for bonuses and salary increases.
- ERIS-TL information collected is intended to ensure that the most senior Departmental executives have access to accurate and up-to-date information as to the incumbency status of all key SES positions. It is also referenced in the course of key Departmental decision-making with regard to executive staffing.
- SES Bonus Pool information collected is intended to ensure the accurate rating, pay adjustment and bonus information of SES employees compiled for the Departmental Executive Resources Board's (DERB) consideration.
- HANS' intended use is for a more efficient and effective program administration for nominating an employee for gold and silver honor awards and a more efficient process of selecting and ranking the nominees.
- webTA is used to track DOC employee's hours; so each employee can be paid or compensated accordingly.
- HMS tracks and reports on the timeliness of the hiring process, and hiring actions initiated by the DOC's Human Resources Operations Center (DOCHROC) in order to provide management metrics on the overall human resources management project for tracking positon vacancy time to fill only.
- CLC Datafeed Database contains sensitive and non-sensitive personnel data for the Federal civilian employee population. DOC is required to provide OPM EHRI data on a monthly basis. EHRI is a collection of human resources, payroll, and training data. The information in EHRI is used to provide HR and demographic information on each Federal civilian employee. Executive Order 13197 empowers the Office of Personnel Management to collect the personnel data in EHRI.

5.2 Describe any potential threats to privacy as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

PPS – High level users have access and the ability to print/share, bonus and other salary related information. SES BP - High level users have access and the ability to print/share, bonus and other salary related information. Employees with access to this system have filled out a rules of behavior document that addresses such behavior. The department as a whole has department wide training on privacy.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X		
DOC bureaus	X		
Federal agencies		X	
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

X	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: • PPS, SES BP, and CLC receives queried reports from NFC Databases via secure file transfer from OHRM • PPS and SES BP application provide encrypted bulk data transfers to NFC for payroll and payment processing information. • PPS and SES BP application provide batch file uploads via encrypted frontend application to Department of Treasury's HR Connect System for payroll and payment processing information. • Data from CLC Datafeed is uploaded to the LMS vendor Cornerstone On Demand through a secured front-end application
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at:	
X	Yes, notice is provided by other means.	Specify how: Once users are logged in to the OHRM applications, they get the message "The data in this system is Privacy Act protected, thus users must obey all agency policies regarding the protection of the data. Privacy Act data must never be shared with anyone who does not have a work-related need to know." (The notice is also on the NFC HR Application Access Request form. The user agrees to the statement before creation of the account)
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Individuals have the opportunity to decline to provide PII/BII. In doing so, they will be ineligible for employment with the Department of Commerce.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: Individuals are not given an opportunity to give consent after the initial HR hiring progress.

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Individuals have an opportunity to update their PII/BII using source systems (EPP, eOPF, or HR Connect, etc.) and are informed of this upon gaining access to these systems.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

X	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Access logs are kept and reviewed for any anomalies
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 8/9/2017 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.

X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
X	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

The PII data used in the OHRM Applications, is NFC data, provided by the Office of Human Resources Management. All PII information is transferred in a secure fashion. Unauthorized use of the system is restricted by user authentication. Access logs are kept and reviewed for any anomalies. To guard against the interception of communication over the Internet, the OHRM Applications use the Secure Socket Layer (SSL) protocol which encrypts communications between users' web browsers and the web server. Data that flows between the web server and the database server is secured through encrypted communication. Data stored in the database is encrypted.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: The OHRM Apps are covered by the system of records notice (SORN) DEPT–1 Attendance, Leave, and Payroll Records of Employees and Certain Other Persons, DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies, OPM/GOVT-1,General personnel Records, OPM/GOVT-2, Employee Performance File System Records, and OPM/GOVT-5, Recruiting, Examining, and Placement Records.
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule.

	Provide the name of the record control schedule: The retention period for these records is guided by the General Records Schedules (GRS), which are issued by the National Archives and Records Administration (NARA) to provide disposition authorization for records common to several or all agencies of the Federal Government. In accordance with GRS 20, item 3, electronic versions of records scheduled for disposal may be deleted at the expiration of the retention period authorized by the GRS for the equivalent paper copies or when no longer needed, whichever is later. Various items in GRS 1, Civilian Personnel Records, authorize the disposition of the records described in this PIA.
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding		Overwriting	X
Degaussing		Deleting	X
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
X	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: The ability to identify specific individuals has been evaluated
X	Quantity of PII	Provide explanation: The PII contained in the various systems is collected from all Commerce Employees

X	Data Field Sensitivity	Provide explanation: Data collected contains various PII including SSN and Financial Information
X	Context of Use	Provide explanation: Data is used to collect time and attendance and provide bonuses to employees
X	Obligation to Protect Confidentiality	Provide explanation: The Privacy Act of 1974 (5 USC 552a) and OMB Memorandum provide the obligation to the US Government to protect this information.
	Access to and Location of PII	Provide explanation:
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

Annually the number of people who have access to privacy information is reviewed. A new process to evaluate each person's access to the systems is being started. At this point there has been no new conversation around the amount or method in which information is collected or the source from which the information is collected.

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:

X	No, the conduct of this PIA does not result in any required technology changes.