U.S. Department of Commerce
Office of the Secretary (OS)

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

Reviewed by: Tiffany Daniel, Bureau Chief Privacy Officer (BCPO)

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

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

☐ Concurrence of the BCPO (This is an existing information system that is eligible for an annual certification)

CHARLES CUTSHALL Digitally signed by CHARLES CUTSHALL
Date: 2025.02.27 14:26:42 -05'00'

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date
(Or the BCPO if this is an existing system that is eligible for an annual certification)

U.S. Department of Commerce
Office of the Secretary
Office of Human Resources Management (OHRM) Applications

Privacy Impact Assessment

Unique Project Identifier: An EAS OS-059 Sub-Application

<u>Introduction</u>: System Description

Provide a brief description of the information system.

The Office of Human Resources Management (OHRM) Applications are responsible for planning, developing, administering, and evaluating the human resources (HR) 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. OHRM is comprised of the Automated Classification System (ACS), the Access Management Portal (AMP), the Executive Resource Information System-Top Level (ERIS-TL), the Honor Award Nominee System (HANS), the Performance Payout System (PPS), Senior Executive Service Bonus Pool (SES BP), and the Commerce Learning Center (CLC) Datafeed. These systems are all covered in this PIA.

Address the following elements:

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

OHRM Apps are categorized as a minor application.

(b) System location

The systems are primarily managed by resources located in the Commerce Business System (CBS) Solution Center (CSC) in Gaithersburg, MD. The system is physically located at the Department of Transportation – Enterprise Services Center (DOTESC) 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 payroll and payment processing, HR personnel data files from OHRM's PPS and SES BP, are manually batched to the US Department of Agriculture
(USDA) National Finance Center (NFC) database. A second file is uploaded to the Department of the Treasury's HR Connect System for department wide all-in-one front-end

HR system. The files are retrieved by a designated member of Enterprise Services and the OHRM NFC Liaison through the HR application and/or Kiteworks.

Data from CLC Datafeed is uploaded to the Learning Management System (LMS) vendor Cornerstone On-Demand, as a part of their user integration application.

OHRM also obtains data from USDA for PPS, CLC Datafeed, and the SES Bonus Pool, which is sent through the aforementioned bi-weekly reports from NFC, via Kiteworks from OHRM's NFC liaison.

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

The OHRM Applications utilize a wide variety of Human Resource (HR) systems to provide Department-wide human resources services. These applications, introduced in the above system description, perform vital functions to support OHRM business. These systems are accessed through the OHRM AMP. Users are granted access to the appropriate system within the AMP based on approval from their immediate supervisor and the system Administrator. The specific type of PII processed by each system is included in Section 2. The data is transmitted to NFC via the process described in section C.

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.

AMP is designed to manage users across all five applications (ACS, ERIS-TL, HANS, PPS, and SES BP) and provide authorization and authentication processes for end users to access each application, user account maintenance, password maintenance and recovery.

ERIS-TL is designed to provide to a limited cadre of the most senior Commerce executives information regarding the incumbency status of all key positions to aid in executive level staffing decisions.

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 produces reports including certificate citations, program booklets, and seating charts.

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.

SES BP provides the functionality to record and report the annual performance ratings, performance increases, and bonus recommendations, and calculate the ACIs for the SES employees and transmit the updated data to NFC as previously described in section C.

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 the HR Systems. 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 operating unit 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 operating unit and DOC

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

Information is transmitted across approved encryption protocols such as Hypertext Transfer Protocol Secure (HTTPS) and Secure Shell (SSH). Sensitive data transmissions are encrypted according to NIST 800-18, Federal Information Processing Standards (FIPS) 186-4, Digital Signature Standard and FIPS 180-4, and Secure Hash Standard issued by NIST when necessary.

(g) Any information sharing

No information sharing is performed outside of the instances described in section C.

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

The following programmatic authorities, with all revisions and amendments, apply to the systems covered in this PIA: ACS, AMP, ERIS – TL, HANS, PPS, SES BP, and the CLC Datafeed.

System	Authorities
ACS	5 U.S.C. 301; 44 U.S.C. 3101; Executive Order (E.O.) 12107; Executive Order (E.O.) 13197; 41U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-430: Performance Management System; DAO 202-450: Delegation of Authority for Human Resources Management; DOO 20-8: Director for Human Resources Management - SECTION 4.

AMP	5 U.S.C. 301; 44 U.S.C. 3101; Executive Order (E.O.) 12107; Executive Order (E.O.) 13197; 41U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-430: Performance Management System; DAO 202-450: Delegation of Authority for Human Resources Management; DOO 20-8: Director for Human Resources Management - SECTION 4.
ERIS-TL	5 U.S.C. 301; 44 U.S.C. 3101; Executive Order (E.O.) 12107; Executive Order (E.O.) 13197; 41U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-430: Performance Management System; DAO 202-450: Delegation of Authority for Human Resources Management; DOO 20-8: Director for Human Resources Management - SECTION 4.
HANS	5 U.S.C. 301; 44 U.S.C. 3101; Executive Order (E.O.) 12107; Executive Order (E.O.) 13197; 41U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-430: Performance Management System; DAO 202-450: Delegation of Authority for Human Resources Management; DOO 20-8: Director for Human Resources Management - SECTION 4.
PPS	5 U.S.C. 301; 44 U.S.C. 3101; Executive Order (E.O.) 12107; Executive Order (E.O.) 13197; 41U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-430: Performance Management System; DAO 202-450: Delegation of Authority for Human Resources Management; DOO 20-8: Director for Human Resources Management - SECTION 4.
SES BP	5 U.S.C. 301; 44 U.S.C. 3101; Executive Order (E.O.) 12107; Executive Order (E.O.) 13197; 41U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-430: Performance Management System; DAO 202-450: Delegation of Authority for Human Resources Management; DOO 20-8: Director for Human Resources Management - SECTION 4.
CLC Datafeed	5 U.S.C. 301; 44 U.S.C. 3101; Executive Order (E.O.) 12107; Executive Order (E.O.) 13197; 41U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-430: Performance Management System; DAO 202-450: Delegation of Authority for Human Resources Management; DOO 20-8: Director for Human Resources Management - SECTION 4.

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

OHRM is classified as a MODERATE application.

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 Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

__X_ 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.

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

__ __ This is an existing information system that is eligible for an annual certification, in which security and privacy controls are properly implemented, 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	f. Driver's License		j. Financial Account	
b. Taxpayer ID		g. Passport		k. Financial Transaction	
c. Employer ID	X	h. Alien Registration		l. Vehicle Identifier	
d. Employee ID		i. Credit Card		m. Medical Record	
e. File/Case ID					
n. Other identifying numbers (specify):					
*Explanation for the business 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. It is collected only by the PPS, SES BP, and CLC Datafeed.					

General Personal Data (GPD)					
a. Name	X	h. Date of Birth	X	o. Financial Information	X
b. Maiden Name		i. Place of Birth		p. Medical Information	
c. Alias		j. Home Address	X	q. Military Service	
d. Gender	X	k. Telephone Number	X	r. Criminal Record	
e. Age	X	l. Email Address	X	s. Marital Status	
f. Race/Ethnicity	X	m. Education	X	t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify): The GPD specified is collected by PPS, SES BP, and the CLC Datafeed.					

Work-Related Data (WRD)					
a. Occupation	X	e. Work Email Address	X	i. Business Associates	
b. Job Title	X	f. Salary	X	j. Proprietary or Business Information	
c. Work Address	X	g. Work History	X	k. Procurement/contracting records	
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information	X		
l. Other work-related data (specify): Salary, bonus, pay increase information, series, grade, and Entrance on Duty (EOD) date. All OHRM systems contain this work-related data.					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		f. Scars, Marks, Tattoos		k. Signatures	
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording		h. Eye Color		m. DNA Sample or Profile	
d. Video Recording		i. Height		n. Retina/Iris Scans	
e. Photographs		j. Weight		o. Dental Profile	
p. 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	f. 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):					

Government Sources					
Within the Operating unit	X	Other DOC Operating units	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. The data is distributed to OHRM via Kiteworks secure file transfer. Information is not altered by the CBS Solutions Center (CSC) staff. Top Level, HANS, and ACS, information is directly inputted by the authorized users of the system and not CSC resources. Audit logs confirm input into the system.

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		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):			

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 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 during key Departmental decision-making regarding 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.
- CLC Datafeed Database contains sensitive and non-sensitive personnel data for the Federal civilian employee population. DOC is required to provide the Office of Personnel Management (OPM) Enterprise Human Resources Integration (EHRI) data monthly. 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 OPM to collect the personnel data in EHRI.

The specified PII/BII collected by these systems is in reference to federal employees and contractors.

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the operating unit's use of the information, and controls that the 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.)

There is a potential for insider threat to OHRM.

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 has department wide training on Cybersecurity and Privacy Awareness, which is an annual requirement.

Any data with PII is provided via Kiteworks. That information is downloaded to a secure location with a limited number of people with access. Downloads are disposed of/deleted when no longer needed or due to the data retention policy.

Section 6: Information Sharing and Access

6.1 Indicate with whom the operating unit 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 operating unit	X		
DOC operating units	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 Does the DOC operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

X	Yes, the external agency/entity is required to verify with the DOC operating unit before re-dissemination of PII/BII.
	No, the external agency/entity is not required to verify with the DOC operating unit before re-dissemination of PII/BII.
	No, the operating unit does not share PII/BII with external agencies/entities.

6.3 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: External agencies/entities are required to gain approval prior to re-dissemination of PII/BII shared with the external agency/entity. • PPS, SES BP, and CLC receive queried reports from NFC Databases via secure file transfer from OHRM. • PPS and SES BP application provide encrypted bulk data transfers manually 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.

6.4 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. The OHRM applications are covered by the SORNs listed below. 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	
	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 into 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."

	No, notice is not provided.	Specify why not:

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

	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
X	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: All OHRM applications pull the data from the payroll provider NFC via bulk transfer to OHRM, which means any PII/BII data information has already been collected, maintained and disseminated by the system of record, NFC.

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: All OHRM applications pull the data from the payroll provider NFC via bulk transfer to OHRM, which means any PII/BII data information has already been collected, maintained and disseminated by the system of record, NFC.

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 (Employee Personal Page (EPP), Electronic Official Personnel File (eOPF), or Human Resource Connect (HRC), etc.) and are informed of this upon gaining access to these systems. Data in the source systems is ingested into the systems as described in section C.
	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: Audit logs monitor, track, and record all user actions when handling PII information. Privileged account reviews are conducted quarterly to adhere to least privilege principles.
X	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): _______8/8/2024__________ ☐ 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 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 DOC 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 Is the PII/BII searchable by a personal identifier (e.g., name or Social Security number)?

__X__ Yes, the PII/BII is searchable by a personal identifier.

____ No, the PII/BII is not searchable by a personal identifier.

9.2 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)*: All of the OHRM applications are covered by each of the SORNs listed below. 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
	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: PPS adheres to the Code of Federal Regulations Title 5, Section 293.404-part a. eCFR :: 5 CFR 293.404 -- Retention schedule. SES BP adheres to the Code of Federal Regulations Title 5, Section 293.404-part b. eCFR :: 5 CFR 293.404 -- Retention schedule. ACS, AMP, ERIS-TL, HANS, and CLC Datafeed adhere to GRS 2.2, Item 10. The General Records Schedules as of Transmittal 36 (archives.gov)
	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, and does not have to be 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 level. *(Check all that apply.)*

X	Identifiability	Provide explanation: The ability to identify specific individuals has been evaluated and it was determined to have a high likelihood.
X	Quantity of PII	Provide explanation: The PII contained in the various systems is collected from all Commerce Employees (approximately 50,000)
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 reward information and provide bonus 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 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.)

There is a potential for insider threat to OHRM. Annually the number of people who have access to privacy information is reviewed. Operating unit users have access to review and approve user accounts through the OHRM Account Management Portal.

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.