Template Version Number: 01-2021

U.S. Department of Commerce
U.S. Census Bureau

Privacy Impact Assessment
for the
Office of the Chief Information Officer (OCIO) Human Resources Applications

Reviewed by: _____Byron Crenshaw_____, Bureau Chief 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

TAHIRA MURPHY Digitally signed by TAHIRA MURPHY Date: 2024.11.29 21:57:39 -05'00' for Charles Cutshall 10/31/24

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

U.S. Department of Commerce Privacy Impact Assessment
U.S. Census Bureau/Office of the Chief Information Officer (OCIO)
Human Resources Applications

Unique Project Identifier: 006-000401400

Introduction: System Description

Provide a brief description of the information system.

The Office of the Chief Information Officer (OCIO) Human Resource Applications are a set of systems which collect and manage personnel information for employees and non-employees. Information from these systems is shared with authorized systems through approved interfaces and connections. These set of systems consist of the Census Hiring and Employment Check (CHEC) system, Census Human Resources Information System (CHRIS) and Decennial Applicant Personnel and Payroll System (DAPPS). CHEC processes background checks for employment suitability and manages non-employee personnel information. CHRIS is a suite of workforce management applications used by Human Resource Division, hiring managers, Census Health Unit Staff, contractors, and employees. Field Supervisors and Field Representatives use an application in CHRIS for managing and recording time and expense data for current surveys. DAPPS is a human resource and payroll processing system for decennial temporary hires supporting the recruiting and applicant process, personnel actions, daily time & expense, and payroll activities. The Human Resource applications are internal Census systems within the OCIO security boundary.

Address the following elements:

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

The OCIO Human Resources Applications are major application systems with several subsystem components. These IT systems provide support for internal and external customers in need of automated services for managing applicant/contractor suitability, personnel processing, time tracking, payroll processing, and other administrative activities. The systems are designed to meet the workforce needs of Census Bureau employees and contractors.

(b) System location

The information collected and maintained by the OCIO Human Resources Applications is housed in the Census Bureau Computing Center.

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

The OCIO Human Resources Applications interconnect with other systems both internal and external such as:

- Department of Homeland Security (DHS) – personnel verification.
- Department of the Treasury/HRConnect – HR data, payroll, bank routing data.
- Defense Counterintelligence and Security Agency (DCSA) – fingerprints.
- Federal Bureau of Investigation (FBI) – fingerprints, personal data, criminal records data.
- Office of Personnel Management (OPM) – recruiting data, health benefits, flexible spending account data.
- National Finance Center (NFC) – payroll, HR, awards, and performance rating data.
- Department of Commerce – GovTA data, personal data, investigation data.
- Social Security Administration (SSA) – HR data.
- Several external vendors (private sector):
    - FedPoint – Federal Long Term Care Insurance data.
    - EQUIFAX – unemployment compensation data.
    - Everbridge via Department of Commerce connection – Emergency contact information.
- Other internal Census Bureau systems: OCIO Commerce Business Systems, OCIO Data Communications Identify Management System, OCIO Client Support Division, Associate Director for Decennial Census Programs (ADDCP) Geography systems and ADDCP Decennial systems.
- Tax data is also shared with the IRS, state, and local municipalities, as required by law.

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

CHEC: The Census Hiring and Employment Check (CHEC) system automates the electronic processing of personnel security data in support of employment suitability and background investigations, managing the onboarding process for Census Bureau employees (i.e., decennial, non-decennial, regional office, NPC), and non-employees (contractors, ancillaries, and special sworn employees), as well as managing the life cycle of non-employees (i.e., contractors, ancillaries and special sworn employees).

CHRIS: The Census Human Resources Information System (CHRIS) is a suite of workforce management applications. CHRIS is key in helping employees keep track of all human resources-related information such as emergency contact information, training history and personnel action history. Employees also use CHRIS to apply for telework and remote work.

CHRIS contains other components used by OCIO Human Resources Division and hiring managers such as Mixed Tour, the Electronic Hiring System (used to hire schedule A and veterans), the Census Awards Recognition System, and the Performance Evaluation and Recognition System. CHRIS also houses the time and expense system, webFred used to track the hours worked and expenses charged by Field Representatives working on current surveys.

The Census Health System (CHS) is also a component of the CHRIS system; any services provided by the Census Health Unit to employees, contractors or other visitors in the building are charted and managed by Census Health Unit staff via CHS. HRD and Administrative Officers also use Entry on Duty and Accessions Forms Tracking for tracking the forms and onboarding status of employees. Personnel action requests are entered in the Personnel Action Request System. Employee Relations, Labor Relations, Harassment Tracking, and Inspector General Tracking Systems are used to manage case information related to grievances, EEO complaints and performance-related issues. The New Hire Tracking system is used by Regional Office personnel as the primary source for tracking new hires working in Special Censuses and surveys. The Employee Assistance Program (EAP) system allows users to create, process, refer, and close EAP cases. The Incident Tracking System provides the ability to record, track, manage and report incidents related to safety issues, physical security events, IT security events, and possible data breaches. The BC-282 application is used by Field Division to document conduct and or performance problems. The Employee Designation application allows users with access to manage (add, edit, and remove) employee designations such as Capstone Officials, COOP Excepted Part-Time, Excepted Full-Time, etc.

DAPPS: The Decennial Applicant Personnel and Payroll System (DAPPS) is a fully integrated human resources and payroll system that meets financial and regulatory reporting requirements for temporary decennial field staff. This web-based enterprise-wide system supports the recruiting and applicant process, creating electronic selection certificates, hiring/rehiring staff, processing personnel actions, entering daily time & expense, running weekly payrolls, creating reports, administering benefits for intermittent employees, and maintaining historical information.

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

Information contained in the OCIO Human Resources information systems are available to authorized Census Bureau federal employees and contractors with need-to-know access to the applications. The information within the OCIO Human Resources Division applications is retrieved using authorized internal web applications, file servers and/or databases that are protected with a multi-layer security approach as identified in the selected security controls for the OCIO Human Resources applications. Individual records are retrieved by name, employee number, or other personal identifier.

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

Information is transmitted to and from the OCIO Human Resources Systems via web services, secure file transfer protocol (SFTP), and the Cumulus API Gateway

(g) Any information sharing

The OCIO Human Resource Systems share information internally with OCIO Commerce Business Systems (CBS), ADDCP Geographic Systems, and ADDCP Decennial and externally

with other federal agencies, state and local governments, the Department of Commerce and private vendors (Everbridge, Equifax, and FedPoint) as described in item *(c)*.

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

5 U.S.C. 301, 44 U.S.C. 3101, and 3309, 5 U.S.C. 7531-332

5 U.S.C., 5379, 5 CFR Part 537,

5 U.S.C. 1302, 2951, 3301, 3372, 4118, and 8347

5 U.S.C. 1104, 3321, 4305, and 5405

5 U.S.C. 3321, 4303, 7504, 7514, and 7543

5 U.S.C. 309, 3109, 3302, 3304, 3305, 3306, 3307, 3313, 3317, 3318, 3319, 3326, 4103, 4723, 5532, and 5533

5 U.S.C. 7201, sections 4A, 4B, 15A (1) and (2), 15B (11), and 15D (11)

5 U.S.C. Chapters 11, 33, and 63

5 U.S.C. 7901, Public Law 79-568

5 U.S.C. § 552a(b)(3)

44 USC 3556

Public Law 99-570 (5 U.S.C. 7361 and 7362)

Public Laws 96-180 and 96-181

Public Law 79-658

Executive Order 12564

42 CFR Part 2

29 Code of Federal Regulations (CFR) Part 1614

Equal Employment Opportunity Commission Management Directive 110.

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

The overall security impact category for the OCIO Human Resources Applications is 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 Management Changes		f. Commercial Sources		i. Alteration in Character 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	f. Driver's License	X	j. Financial Account	X
b. Taxpayer ID	X	g. Passport	X	k. Financial Transaction	X
c. Employer ID	X	h. Alien Registration	X	l. Vehicle Identifier	
d. Employee ID	X	i. Credit Card		m. Medical Record	X
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 is required for tax reporting, enrollment for health/life insurance/long-term care/flexible spending benefits etc., background investigations, criminal background records, employee verifications through E-Verify, unemployment compensation and USA staffing through USAJobs.					

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

Work-Related Data (WRD)					
a. Occupation	X	e. Work Email Address	X	i. Business Associates	X
b. Job Title	X	f. Salary	X	j. Proprietary or Business Information	X
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):					

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

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

Non-government Sources					
Public Organizations		Private Sector	X	Commercial Data Brokers	
Third Party Website or Application			X		
Other (specify): The OCIO Human Resources applications contract the services of vendors and contractors for dissemination of data for compliance with local, state and federal laws					

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

The OCIO Human Resource Systems employ a multitude of security controls mandated by the Federal Information Security and Modernization Act of 2014 (FISMA) and various other regulatory control frameworks including National Institute of Standards and Technology (NIST) special publications 800 series. These security controls identified include but are not limited to data validation controls to ensure accuracy of information. Mechanisms such as double entry, system edits, multiple reviews and automated processes are used to ensure accuracy in the information systems. New hires provide required identification documents that is cross-referenced with data input in the human resource systems and its components.

2.4 Is the information covered by the Paperwork Reduction Act?

X	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. 0607-0139, 0607-0139,1530-0006,3206-0142,2550-0001, 3206-0001 0607-0452, 3206-0182, 3206-4182, 1615-0047
	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		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): To maintain minimal medical records for Census Bureau Health Unit visits			

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).

For administering Human Resources (HR) programs: The agency will use the information collected to administer OCIO Human Resources (HR) programs. For example, the system collects performance related information on employees, employees' supervisor, employee rating information, and comments related to performance. Once hired, the information is used to manage personnel and payroll records. The information in this system is vital to keep track of and disseminate Census Bureau employee's HR/payroll transactions.

The OCIO Human Resources applications also collect/maintain data from USA Jobs job applicants, job offers, and collects employee-competency proficiency data (the knowledge, skills, and abilities) needed to perform.

For administrative matters: The information is used to run background investigations of applicants, which include members of the public, federal employees, contractors, and foreign nationals, to provide staffing for the Census Bureau.

To maintain minimal medical records for Census Bureau Health Unit visits:

The medical information collected/maintained in the OCIO Human Resources applications is in reference to Federal employees, contractors, and visitors.

5.2 Describe any potential threats to privacy, such as insider threat, 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.)

The U.S. Census Bureau use of data/information presents possible threats such as internal breaches caused by employees within an organization. Today's most damaging security threats are not originating from malicious outsiders or malware but from trusted insiders - both malicious insiders and negligent insiders. Inside threats are not just malicious employees that intend to directly harm the Bureau through theft or sabotage. Negligent employees can unintentionally cause security breaches and leaks by accident. To prevent or mitigate potential threats to privacy the U.S. Census Bureau has put into place mandatory training for all system users. All Census Bureau employees and contractors undergo mandatory annual data stewardship training to include proper handling, dissemination, and disposal of BII/PII/Title 13/Title 26 data.

In addition, the Census Bureau Information technology systems employ a multitude of layered security controls to protect PII/BII at rest, during processing, as well as in transit. These NIST 800-53 controls, at a minimum, are deployed and managed at the enterprise level, including, but not limited to the following:

- Intrusion Detection | Prevention Systems (IDS | IPS)
- Firewalls
- Mandatory use of HTTP(S) for Census Bureau Public facing websites

- Use of trusted internet connection (TIC)
- Anti-Virus software to protect host/end user systems
- Encryption of databases (Data at rest)
- HSPD-12 Compliant PIV cards
- Access Controls

The Census Bureau Information technology systems also follow the National Institute of Standards and Technology (NIST) standards including special publications 800-53, 800-63, 800-37 etc. Any system within the Census Bureau that contains, transmits, or processes BII/PII has a current authority to operate (ATO) and goes through continuous monitoring on a yearly basis to ensure controls are implemented and operating as intended. The Census Bureau also deploys a Data Loss Prevention solution and a security operations center to monitor all Census IT system on a 24/7/365 basis.

The information in the OCIO Human Resources applications is handled, retained, and disposed of in accordance with appropriate federal record schedules. All Census Bureau buildings have physical security and entry requires a valid form of identification such as the agency issued employee badge.

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	X	X
DOC bureaus	X	X	X
Federal agencies	X	X	X
State, local, tribal gov't agencies	X	X	X
Public			
Private sector		X	
Foreign governments			
Foreign entities			

Other (specify):			

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

6.2 Does the DOC bureau/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 bureau/operating unit before re-dissemination of PII/BII.
	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the bureau/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:
	
	The OCIO Human Resources Applications interconnect with other systems both internal and external such as:
	
	• Department of Homeland Security (DHS) – personnel verification.
	• Department of the Treasury/HRConnect – HR data, payroll, bank routing data.
	• Defense Counterintelligence and Security Agency (DCSA) – fingerprints.
	• Federal Bureau of Investigation (FBI) – fingerprints, personal data, criminal records data.
	• Office of Personnel Management (OPM) – recruiting data, health benefits, flexible spending account data.
	• National Finance Center (NFC) – payroll, HR, awards, and performance rating data.
	• Everbridge via Department of Commerce connection – Emergency contact information.
	• Department of Commerce – GovTA data, personal data, investigation data.
	• Social Security Administration (SSA) – HR data.
	• Several external vendors (private sector):
	  ○ FedPoint – Federal Long Term Care Insurance data.
	  ○ EQUIFAX – unemployment compensation data.
	• Other internal Census Bureau systems: OCIO Commerce Business Systems, OCIO Data Communications Identify Management System, OCIO Client Support Division , Associate Director for Decennial Census Programs (ADDCP) Geography systems and ADDCP Decennial systems.
	• Tax data is also shared with the IRS, state, and local municipalities, as required by law.
	
	The OCIO Human Resource Systems share information internally with OCIO Commerce Business Systems (CBS), ADDCP Geographic Systems, and ADDCP Decennial and externally with other the Department of Commerce, federal agencies, state and local governments, and private vendors (Everbridge, Equifax, and FedPoint).
	
	The system uses a multitude of security controls mandated by the Federal Information Security Modernization Act of 2014 (FISMA) and various other regulatory control frameworks including the National Institute of Standards and Technology (NIST) special publication 800 series. These security controls include but are not limited to the use of mandatory HTTPS for public facing websites, access controls, anti-virus solutions, enterprise auditing/monitoring, encryption of data at rest, and various physical controls at Census facilities that house Information Technology systems. The Census Bureau also

	deploys a Data Loss Prevention solution and a security operations center to monitor all Census IT system on a 24/7/365 basis. Cryptographic mechanisms used to protect data at rest and in transit is in accordance to FIPS 140-2 standards.
	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.	
X	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: https://www.census.gov/about/policies/privacy/privacy-policy.html	
	Yes, notice is provided by other means.	Specify how:
	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 by failing to complete the pre-employment forms. In doing so, they will be ineligible for employment with the Census Bureau. Individuals can decline at the CHRIS level to not share emergency contact information by not providing their emergency contact information in CHRIS.
	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.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: Consent is included on all personnel forms that employees complete, and consent to the uses explained on the forms is implied by completion of the forms. Individual can choose to not consent to the use of their emergency contact information at the CHRIS level by not providing their emergency contact information in CHRIS.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: an opportunity to consent to uses.

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 are able to update personnel and emergency contact and other information using appropriate procedures and HRD applications. Individuals can choose to update their PII via CHRIS. Non-employees can choose to update their PII via CHEC.
	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: Only authorized government/contractor personnel are allowed to access PII within a system. Authorizations for users occur yearly, at a minimum in accordance with applicable Bureau, Agency, and Federal policies/guidelines. In additional to system processes that handle PII/BII, all manual extractions for PII/BII are logged and recorded per Department of Commerce Policy, the NIST 800-53 Appendix J Privacy Control Catalog, and specifically NIST control AU-03, Content of Audit records.
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): _____ July 18, 2023_____ ☐ 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.
	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 OCIO Human Resources applications follow the Census Bureau Information Security policies in protecting PII/BII on the IT systems.

The Census Bureau Information technology systems employ a multitude of layered security controls to protect PII at rest, during processing, as well as in transit. These NIST 800-53 controls, at a minimum, are deployed and managed at the enterprise level including, but not limited to the following:

- Intrusion Detection | Prevention Systems (IDS | IPS) Firewalls
- Mandatory use of HTTP(S) for Census Public facing websites Use of trusted internet connection (TIC)
- Anti-Virus software to protect host/end user systems Encryption of databases (Data at rest)
- HSPD-12 Compliant PIV cards
- Access Controls

The Census Bureau Information technology systems also follow the National Institute of Standards and Technology (NIST) standards including special publications 800-53, 800-63, 800-37 etc. Any system within the Census Bureau that contains, transmits, or processes BII/PII has a current authority to operate (ATO) and goes through continuous monitoring on a yearly basis to ensure controls are implemented and operating as intended. The Census Bureau also deploys a Data Loss Prevention solution and a security operations center to monitor all Census IT system on a 24/7/365 basis.

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)*: COMMERCE/DEPT-1: Attendance, Leave, and Payroll Records of Employees and Certain Other Persons, https://www.commerce.gov/opog/privacy/SORN/SORN-DEPT-1 COMMERCE/DEPT-13: Investigative and Security Records, https://www.commerce.gov/opog/privacy/SORN/SORN-DEPT-13 COMMERCE/DEPT-14: Litigation, Claims, and Administrative Proceeding Records, https://www.commerce.gov/opog/privacy/SORN/SORN-DEPT-14 COMMERCE/DEPT-18: Employees Personnel Files Not Covered by Notices of Other Agencies, https://www.commerce.gov/opog/privacy/SORN/SORN-DEPT-18 COMMERCE/DEPT-19: Mailing Lists, https://www.commerce.gov/opog/privacy/SORN/SORN-DEPT-19 OPM/GOVT-1: General Personnel Records, https://www.opm.gov/information-management/privacy-policy/sorn/opm-sorn-govt-1-general-personnel-records.pdf OPM/GOVT–2: Employee Performance File System Records, https://www.opm.gov/information-management/privacy-policy/sorn/opm-sorn-govt-2-employee-performance-file-system-records.pdf OPM GOVT-3: Records of Adverse Actions, Performance Based Reduction in Grade and Removal Actions, and Termination of Probationers, https://www.opm.gov/information-management/privacy-policy/sorn/opm-sorn-govt-3-records-of-adverse-actions-performance-based-reductions-in-grade-and-removal-actions-and-terminations-of-probationers.pdf OPM/GOVT-5: Recruiting, Examining, and Placement Records, https://www.opm.gov/information-management/privacy-policy/sorn/opm-sorn-govt-5-recruiting-examining-and-placement-records.pdf OPM/GOVT-7: Applicant Race, Sex, National Origin, and Disability Status Records, https://www.opm.gov/information-management/privacy-policy/sorn/opm-sorn-govt-7-applicant-race-sex-national-origin-and-disability-status-records.pdf OPM/GOVT-10: Employee Medical File System Records, https://www.commerce.gov/sites/default/files/opog/OPM-GOV-10-employee-medical-file-systems-records.pdf EEOC/GOVT–1: Equal Employment Opportunity in the Federal Government Complaint and Appeal Records https://www.commerce.gov/sites/default/files/opog/EEOC-GOV1-18895.pdf
	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: GRS 1 Item 23 Employee Performance File System Records; GRS 2 Item 1 Individual Employee Pay Record GRS 2 Item 8 Individual Employee Pay Record Time and Attendance Input Records GRS 3.1: General Technology Management Records GRS 3.2: Information Systems Security Records GRS 4.2: Information Access and Protection Records GRS 4.3: Input Records, Output Records, and Electronic Copies
	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	X	Overwriting	
Degaussing	X	Deleting	
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: PII/BII collected can be directly used to identify individuals
X	Quantity of PII	Provide explanation: The collection is for Census Bureau human resource systems, therefore, a severe or catastrophic number of individuals would be affected if there were loss, theft or compromise of the data.
X	Data Field Sensitivity	Provide explanation: The PII, alone or in combination, are directly usable in other contexts and make the individual or organization vulnerable to harms, such as identity theft, embarrassment, loss of trust, or costs.
X	Context of Use	Provide explanation: Disclosure of the PII itself is likely to result in severe or catastrophic harm to the individual or organization such as background investigations, criminal background records, employee verifications through E-Verify, unemployment compensation, etc.…
X	Obligation to Protect Confidentiality	Provide explanation: PII collected is required to be protected in accordance with organization or mission- specific privacy laws, regulations, mandates, or organizational policy apply that add more restrictive requirements to government- wide or industry-specific requirements. Violations may result in severe civil or criminal penalties.
X	Access to and Location of PII	Provide explanation: PII is located on computers controlled by the Census Bureau or storage media. Access is limited to certain staff of the Census Bureau's workforce and limited to Special Sworn Status individuals. Access is only allowed by organization-owned equipment outside of the physical locations, and only with a secured connection.
	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.)

Although this IT system can only be accessed by authorized individuals that have a business need to know, the potential risk from insider threat to the organization, which may cause harm such as identity theft, embarrassment, loss of trust, or cost, still exists. The Census Bureau conducts routine security awareness training on recognizing and reporting potential indicators of insider threat. Insider threat is always possible.

In addition, the Census Bureau Information technology systems employ a multitude of layered security controls to protect PII/BII at rest, during processing, as well as in transit. These NIST 800-53 controls, at a minimum, are deployed and managed at the enterprise level, including, but not limited to the following:

- Intrusion Detection | Prevention Systems (IDS | IPS)
- Firewalls
- Mandatory use of HTTP(S) for Census Bureau Public facing websites
- Use of trusted internet connection (TIC)
- Anti-Virus software to protect host/end user systems
- Encryption of databases (Data at rest)
- HSPD-12 Compliant PIV cards
- Access Controls

The Census Bureau Information technology systems also follow the National Institute of Standards and Technology (NIST) standards including special publications 800-53, 800-63, 800-37 etc. Any system within the Census Bureau that contains, transmits, or processes BII/ PII has a current authority to operate (ATO) and goes through continuous monitoring on a yearly basis to ensure controls are implemented and operating as intended. The Census Bureau also deploys a Data Loss Prevention solution and a security operations center to monitor all Census IT system on a 24/7/365 basis.20

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.