Template Version Number: 01-2020

U.S. Department of Commerce
Office of Secretary

Privacy Impact Assessment
for the
Human Resources Management System (HR Connect)

Reviewed by: Maria D. Dumas, 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

JENNIFER GOODE Digitally signed by JENNIFER GOODE
Date: 2021.10.21 13:26:58 -04'00' 10/21/2021

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

U.S. Department of Commerce Privacy Impact Assessment
Human Resources Management System (HR Connect)

Unique Project Identifier: [Number]

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 HR Connect system is an integrated human resource enterprise solution, owned by the U.S. Department of the Treasury (Treasury) and leveraged by the Department of Commerce (DOC or "the Department"), and other Federal agencies, pursuant to the U.S. Office of Personnel Management (OPM) Human Resources Line of Business (HRLOB).

An Interconnection Security Agreement (ISA), which governs the use of the HR Connect application, is countersigned by the Servicing Agency (Treasury) and the DOC, and an Interagency Agreement (IAA), documents the services provided to DOC by Treasury. Additionally, a Service Level Agreement (SLA) outlines the providing of services, including HR Connect, to the DOC by Treasury. HR Connect consists of a General Support System (GSS), a Major Application (MA) and a set of constituent components.

(b) System location

HRConnect consists of a general support system (GSS) and a Major Application (MA) (also known as PaaS and SaaS); customized PeopleSoft HR software residing on the Oracle Cloud Infrastructure's GovCloud Infrastructure as a Service (IaaS) Cloud Service Provider (CSP).

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

HR Connect does not interconnect with or directly interface with any DOC systems. This interconnection is limited to allowing authorized DOC users access to HR Connect from DOC networks. The Enterprise Services (ES) HRServiceNow systems receive nightly basis bulk data extracts and processes the data extracted from HR Connect, which are manually uploaded to HRServiceNow to support that system's core functionality.

The Treasury HR Connect system shares an interconnection with the Department of Agriculture's National Finance Center (NFC) Payroll/Personnel System (PPS) for the delivery of automated human resources operations. Additional information on this connection is available in the Treasury Privacy and Civil Liberties Impact Assessment for the HR Connect system.

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

In 2010, DOC implemented a Human Resources Management System (HRMS) that complies with OPM's Human Resources Line of Business (HRLOB) model. DOC's vision for the HRMS was to provide an Agency-wide, modern, cost- effective, standardized, and interoperable HR solution that delivers common, core functionality to support the strategic management of human capital and addresses the manual and inefficient processing of HR transactions, by leveraging OPM guidance on the Shared Service Center (SSC) model, DOC evaluated the six OPM certified public sector SSCs and identified Treasury's HR Connect as its preferred provider.

From a business perspective, DOC's decision to migrate its Servicing HR Organizations (HRSO) to an HRLOB (and specifically HR Connect) mandated that all DOC bureaus co-exist in one standard software code line, ending a DOC history of HR system autonomy through varied implementations of other legacy HR systems and traditional paper-based processing across its Bureaus, offices, and Operating Units.

HR Connect supports the common HRLOB processes and provides core HR functionality to include: Administering Benefits, Employee/Labor Relations case tracking, Managing Payroll, Organization and Position Management, Personnel Action Processing, Separation Management, and Staff Acquisition.

To facilitate these common HRLOB processes, HR Connect collects and maintains Personally Identifiable Information (PII). PII in the system is used by DOC to:

- Record deductions, leave accrued and taken; maintain and display leave and earnings statements; commence and terminate allotments; answer inquiries; and process claims;
- Maintain current and historical personnel records and prepare individual administrative transactions relating to education and training, job assignment, career development, evaluation, promotion, compensation, separation, and retirement;
- Provide data to produce reports, statistical surveys, rosters, documentation, and studies required for orderly personnel administration within Treasury;

- Maintain and administer organizational setup, such as organizational hierarchy; reporting hierarchy; job codes and classification; pay plans and associated salary (including locality pay); work locations; and position budget management; and

Perform personnel functions for Federal agencies for which Treasury is a cross-services provider and provide information necessary to enable the payroll provider, NFC, to perform the activities necessary to calculate and distribute pay.

PII is collected from DOC employees, managers, HR professionals and contractors.

The Department previously addressed its use of HR Connect in a Privacy Impact Assessment. Though Treasury owns and operates the system, the Department decided to conduct its own risk assessment in the interest of transparency. This PIA replaces the previously published PIA and has been updated to reflect the DOC's current use of HR Connect, as well as the transfer of certain HR functions to the Department's Enterprise Services organization.

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

Data is retrievable by personal identifier or by social security number (SSN). Data can be retrieved either by the employee identifier or SSN as it pertains to an individual, or by the name of the employee if the information is being retrieved by either the manager of record or in the case on contractors/consultants, by the manager of the contract.

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

Applicants who receive and accept job offers for employment with the DOC, submit information using the forms listed in Table 1 below, which are required to complete the hiring/on-boarding process.

Form Number	Form Name
AD-349	Employee Address
D4A	DC Tax Waiver
DG 60	Federal Employee Health Benefit Conversion Waiver
DS5002	Foreign Service Designation of Beneficiary Form
I-9	Employment Eligibility Verification
OF-306	Declaration for Federal Employment
OGE-278e	Executive Branch Personnel Public Financial Disclosure Report
OGE 450	Confidential Financial Disclosure
N/A	PIV Applicant Information
SF-50	Notification of Personnel Action
SF-61	Appointment Affidavit/Oath of Office
SF-144	Statement of Prior Federal Service
SF-181	Ethnicity and Race Identification
SF-256	Self-Identification of Disability
SF-1152	Designation of Beneficiary Unpaid Compensation
SF-1199A	Direct Deposit
SF-2808	Designation of Beneficiary – Civil Service Retirement System (CSRS)
SF-2809	Health Benefits Election Form
SF-2817	FEGLI Life Insurance Election
SF-2823	FEGLI Designation of Beneficiary
SF-3109	Federal Employees Retirement System (FERS) Election of Coverage
SF-3102	Designation of Beneficiary – Federal Employees Retirement System (FERS)
TSP1	Thrift Savings Plan Election Form
TSP1-C	Thrift Savings Plan Catch-Up
TSP3	Designation of Beneficiary
TSP-19	Transfer
W-4	Federal Tax Withholding
Various	State tax Withholding

The Treasury HR Connect data submitted is manually entered by DOC Human Resources (HR) professionals for purposes of performing activities related to individuals' employment, such as compensation, benefits, and retirement.

Additionally, PII relating to government contractors and consultants comes directly from a source designated as the contracting office (CO or COR) or the contracting officer technical representative (COTR) and includes employee identification and status data such as name, records that establish an individual's identity, Social Security number (SSN), date of birth, sex, race and national origin.

The data stored in HR Connect is processed nightly to the National Finance Center (NFC), the Department of Commerce's payroll System of Record. Information is then returned from the NFC to HR Connect. This includes information regarding national ID (SSN), job data, compensation data, location information, etc. Additionally, data is disseminated from the system via reports and extracts, which are then used to support DOC HR processes or feed existing DOC HR systems.

HR Connect has numerous reports built into its system and data is also defined in Workforce Analytics. Workforce Analytics is an ad hoc reporting tool which includes information on the employee, job, position, and performance related information. Access to various reports is based on system security roles and "need to know" criteria as outlined in this PIA.

Employee related data is available to managers and HR professionals within DOC for effective workforce administration: for example, the processing of personnel actions, roster, employee location, not to exceed

(NTE) dates, emergency contacts, pending and processing actions, and financial disclosure. Included in HR Reports are inbound interface reports, NFC error listings, manager-initiated actions, group/mass awards, NTE dates, emergency contacts, and other similar information

(g) Any information sharing conducted by the system

As noted above, while HR Connect does not interconnect with other DOC systems, other DOC systems may receive, and process data extracted from HR Connect – for example, the ES HRServiceNow solution receives bulk data extracts from HR Connect, which are manually uploaded to HRServiceNow on a nightly basis to support that system's core functionality. HR Connect shares an interconnection with the NFC's PPS for the delivery of automated human resources operations. Data is sent nightly from HR Connect to the NFC PPS and then returned to HR Connect via secure transmission.

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

- Title 5 U.S.C.
- Title 31 U.S.C. 66a, 492
- Title 44 U.S.C. 3101, 3309
- E.O. 12107
- E.O. 13164
- Homeland Security Presidential Directive 12 (HSPD-12) – requires the development and agency implementation of a mandatory, government-wide standard for secure and reliable forms of identification for Federal employees and contractors.

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

Treasury's HR Connect system is categorized as FIPS 199 High

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 (version 01-2014 or 01-2017).
____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2019 or later).

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	X
b. Taxpayer ID		g. Passport		k. Financial	

				Transaction	
c. Employer ID		h. Alien Registration		l. Vehicle Identifier	
d. Employee ID	X	i. Credit Card		m. Medical Record	
e. File/Case ID	X				
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form: Includes both full and truncated SSNs. The SSN is required by HR Connect's payroll provider, the United States Department of Agriculture, National Finance Center (NFC) to establish identity. NFC has operated as a payroll system of records since 1973 and is therefore exempt from the Privacy Act requirements regarding the collection and use of the SSN.					

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

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		k. Procurement/contracting records	
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information			
l. Other work-related data (specify):					

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	X	f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)
– Employee Emergency Contact Data (name, address, phone number) – Disability Data – Federal & State Tax Data – Beneficiary & Dependent Data – Health Benefit Data

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	X		
Other (specify):					

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.

Data templates are filled out and submitted by dedicated HR data Subject Matter Experts (SMEs) at each of the various operating units within the Department. Treasury then merges the information with current data from NFC to populate HR Connect. Treasury's project team manage the data, as they are responsible for the maintenance of the system, help desk practices, and troubleshooting to solve problems that may arise.

The HR Servicing Operation Centers, through HR SMEs will maintain an employee's HR record in addition to allowing the individual to update their data throughout their employment to keep it current. The currency of the data obtained from a bureau's HR office is subject to their data management business rules.

As noted above, a large portion of data is collected directly from employees themselves, through various forms submitted via the on-boarding process. Data is entered by agency HR Specialist and verified for accuracy and relevancy and then verified through SF50 functionality. Data that is contained in HR Connect is reflective of employee data in NFC; consequently, it will be the employee and the Servicing HR Office (SHRO) at the Bureau, office, or Operating Unit level that will consistently verify that the data is accurate and relevant. Employees have access to their data (though not through HR Connect), so they will share the responsibility of maintaining its accuracy.

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. HR Connect collects information using the forms listed in the Table 1 above, many of which are subject to the Paperwork Reduction Act. A hyperlink for each form has been included to facilitate review of the form, including identifying any applicable OMB control number for that specific form. Please note, that not all forms used for input to HR Connect are subject to PRA requirements (for example, District of Columbia tax withholding exemption (D4-A).
	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):

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).

HR Connect supports the common HRLOB processes – core functions include: Administering Benefits, Employee/Labor Relations case tracking, Managing Payroll, Organization and Position Management, Personnel Action Processing, Separation Management, and Staff Acquisition.

Specifically, PII/BII in the system, is collected from DOC employees, contractors, managers, and HR professionals, and used by the DOC and its partner agencies, as necessary to:

– Record deductions, leave accrued and taken; maintain and display Leave and Earnings statements; commence and terminate allotments; answer inquiries; and process claims;

–Maintain current and historical personnel records and prepare individual administrative transactions relating to education and training; job assignment; career development; evaluation; promotion, compensation, separation and retirement;

–Provide data to produce reports, statistical surveys, rosters, documentation, and studies required for orderly personnel administration within Treasury;

Maintain and administer organizational setup, such as organizational hierarchy; reporting hierarchy; job codes and classification; pay plans and associated salary (including locality pay); work locations; and position budget management;

–Perform personnel functions for Federal agencies for which Treasury is a cross-services provider and provide information necessary to enable the payroll provider, NFC, to perform the activities necessary to calculate and distribute pay

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.)

There are three primary risks associated with the processing of PII in the HR Connect solution, including:

- A risk of physical damage to the data facility where the HR Connect solution is housed – including by water, fire, or hurricane – or of a technical failure of hardware or software used by the system, resulting in a lack of availability of data used in making HR-related decisions;
- A risk of compromise of functions in the system, including error in use, abuse of rights, denial of actions, or other similar compromises leading to lack of availability or integrity of data used in making HR-related decisions; and
- A risk of insider threat, or compromise of information by eavesdropping, media theft, retrieval of discarded materials, or other means, including inadvertent disclosure of information to an incorrect user, resulting in harm, including the potential for identity theft, for impacted persons.

Treasury has implemented all required NIST security controls for a High system and continuously monitors, reassess, and reauthorizes the system (every three years) to ensure the system and its information are appropriately protected. Controls applied and assessed include, but are not limited to, access control, role-based access management, authorization, audit and accountability, configuration management, identification and authentication, and encryption. These controls are further discussed in Section 8.1 and 8.2 below.

An SLA between Treasury and DOC governs management of the system, including appropriate use by DOC personnel. All personnel granted system access are required to sign and abide by "Rules of Behavior" for appropriate system use. Cybersecurity and Privacy Awareness training is also an annual requirement of the Department for all DOC employees.

Additionally, DOC policy and procedure governs appropriate use of the system, and access to sensitive HR PII, by authorized DOC users. All DOC personnel are trained on privacy and security standards and are given access to PII on a "need to know" and the concept of least privilege.

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	
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 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. An SLA and IAA between Treasury and DOC governs management of PII/BII. The DOC operating unit shall remain the owner of any and all data in the system. Treasury is required to verify with the DOC operating unit before re-disseminating 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: HR Connect does not interconnect with or directly interface with any DOC systems. The ES HRServiceNow systems receives nightly basis bulk data extracts and processes the data extracted from HR Connect, which are manually uploaded to HRServiceNow to support that system's core functionality. The Treasury HR Connect system shares an interconnection with the Department of Agriculture's National Finance Center (NFC) Payroll/Personnel System (PPS) for the delivery of automated human resources operations. Additional information on this connection and the controls in place to protect information in transit between the two systems, is available in the Treasury Privacy and Civil Liberties Impact Assessment for the HR Connect system.
	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):			

All access is based on "need-to-know" and the corresponding system access profiles. Access to the data by a user is determined based upon the user profile that is identified under the strict "need to know" criteria and as a function of position. For example, in the case of managers, managers will only have access to the information that is specifically under their direct ownership or strict "need to know" access controls (i.e. employees that report to them) as well as their own PII. Likewise, SHROs will only have access to a set of employees within the Bureau, Operating Unit, or office they support, and as it relates to their specific duties or position.

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.hrconnect.treas.gov/privacy_policy.html Each form which collects information used to populate the HR Connect system includes a Privacy Act Statement or similar privacy notice. A list of the forms and hyperlinks for each form is provided in Table 1 (Introduction (f)). Additional information on the forms, which initially collect information for the system, can be found in Treasury's Privacy and Civil Liberties Impact Assessment for the HR Connect system. Additionally notice is provided in the form of a SF-50 (notification of personnel action) anytime data is updated or changed in the system.	
X	Yes, notice is provided by other means.	Specify how: Additional notice is provided through the Treasury's Privacy and Civil Liberties Privacy Impact Assessment.
	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: Individuals do not have the opportunity to initially decline to provide PII/BII. HR Connect is a front-end interface to NFC and is automatically populated with the NFC data of every individual in the organization. HR Connect is then utilized as an automated, core HR processing tool for the entire DOC. Employees

		have the option (pursuant to bureau level business processes) to either use or not use self-service features offered by their respective Bureau, office, or OU. However, they do not have the option to initially decline providing PII.

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: While employees have the option of accessing their own PII/BII (to review and update), they do not have the opportunity to consent to particular uses of their information. Individuals may access their source HR Records through a variety of means within DOC, to include a self- service capability offered through the Enterprise Services (ES) HR ServiceNow system, or via a Privacy Act request. Direct access to HR Connect by employees for their own records is not permitted.

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: As outlined above, any time a personnel action is completed which changes information in the HR Connect system, a Standard Form (SF) 50 is generated. This notifies the employee of the change to their record(s). Individuals may access their source HR Records through a variety of means within DOC, to include a self-service capability offered through the Enterprise Services (ES) HR ServiceNow system, or via a Privacy Act request. Direct access to HR Connect by employees for their own records is not permitted.
	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.)*

	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: HRC FIPS 199 impact level is HIGH and audit and accountability policy and procedures are Inherited from the Treasury Department IT Security Program. For users access, they must fill out the Treasury Shared Services Center (TSSC) security access request form. Managers also must sign the access request form. The agency HRConnect representative will then sign the form as the final approver before access to HRC is granted.
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): 01/31/2021 ☐ 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.
X	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.
X	Other (specify): MOA and Interconnection agreement govern DOC's use of and access to HR Connect. The MOA outlines security requirements and schedule for assessments (every 3 years).

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).*

Treasury is responsible for maintaining security practices in support of the HR Connect solution, including maintain a current security authorization for the system in accordance with the Federal Information Security Modernization Act (FISMA) and with OMB directives and NIST standards, to include the privacy and security controls outlined under NIST 800-53. A memorandum demonstrating system compliance is provided to all customer agencies, including DOC, on an annual basis. Treasury authorized the HR Connect system to operate on Jan 31, 2020 . Re-authorizations occur every three years, in accordance with Treasury Directive 85-01, IT Security Policy.

In general, HR Connect has multiple security checks built into the system to ensure that privacy safeguards are not abused or bypassed. For example:

- A profiled access approach, where only individuals with an established "need to know" may access only their specific profiled data that is controlled by the system.
- Monitoring by security administrators, of any individual that engages in any unauthorized or malicious behavior within the HR Connect environment.
- System Rules of Behavior, which must be agreed to by users before completing registration for system access. Privileged users are required to annually sign the rules behavior.
- Extensive auditing capabilities, including the ability to review auditing trails related to DOC- specific data.
- Deployment of monitoring tools such as intrusion detection devices and vulnerability scanning tools.
- Entrances to data centers and support organization offices are restricted to those employees who require access.
- Disclosure of information through remote terminals is restricted using passwords and sign-on protocols, which are periodically changed.
- Password complexity requirements, as well as the requirement that passwords be changed every 90 days.

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 COMMERCE/DEPT-25 - Access Control and Identity Management System COMMERCE/DEPT 18 – Employee Personnel Files Not Covered by Notices of Other Agencies OPM/GOVT 1 – General Personnel Records OPM/GOVT 5 – Recruiting, Examining, and Placement Records OPM/GOVT 7 – Applicant Race, Sex, National Origin, and Disability Status Records The system of records notice used by the U.S. Department of Treasury is: Treasury.001 – Treasury Personnel and Payroll System
	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: General Records Schedule (GRS) 1 – Civilian Personnel Records
	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	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: **High:** PII includes direct identifiers, such as full names, unique identifying numbers (SSN), etc.
X	Quantity of PII	Provide explanation: **High:** Includes records of more than 10,000 unique individuals.
X	Data Field Sensitivity	Provide explanation: **High:** Data that if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. This includes both standalone data elements (such as Social Security or Alien Registration number, as well as combinations of data such as name and credit card number. This can also include inherently "private" information, such as sexual orientation or lifestyle information
X	Context of Use	Provide explanation: **Moderate:** Information is

		collected for, or used in the administration of benefits or privileges, or determining eligibility for such, or such information is otherwise used in making determinations about an individual
X	Obligation to Protect Confidentiality	**High:** Explicit promises of confidentiality regarding the information have been conveyed to the subject individual at the time or point of collection, information is classified or otherwise law-enforcement or national-security sensitive, or information is afforded confidentiality from unauthorized disclosure by statute or regulation (e.g. Privacy Act of 1974, HIPPA, OMB), agency-specific (Census, IRS), or industry-specific (GLBA, CIPSEA) obligations.
X	Access to and Location of PII	Provide explanation: **Moderate:** PII is maintained or stored non-locally, to include cloud, on removable media, or at a third-party location, and/or access is limited to internal DOC employees or contractors with a bona-fide need-to-know the information. PII may be structured or unstructured, and may be linked between data fields, data sets, tables, or otherwise "connected" in a way which makes quickly accessing large volumes of sensitive information about a specific individual possible.
	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.)

There is a risk of physical damage to the data facility where the HR Connect solution is housed. Such damage may occur by water, fire, or hurricane – or of a technical failure of hardware or software used by the system, resulting in a lack of availability of data used in making HR-related decisions.

There is a risk of compromise of functions in the system, including error in use, abuse of rights. There may be denial of actions, or other similar compromises leading to lack of availability or integrity of data used in making HR-related decisions. Treasury has implemented all required NIST security controls for a High system and continuously monitors, reassess, and reauthorizes the system (every three years) to ensure the system and its information are appropriately protected. Controls applied and assessed include, but are not limited to, access control, role-based access management, authorization, audit and accountability, configuration management, identification and authentication, and encryption.

Any data consolidation that occurs is protected under statutory controls, such as the Privacy Act, configuration management controls, security controls, profiles and access controls in conjunction with the "need-to-know" principles for data protection.

There is a risk that A risk of insider threat, or compromise of information by eavesdropping, media theft. There is a possibility of discarded materials, as an example, or other means, including inadvertent disclosure of information to an incorrect user, resulting in harm, including the potential for identity theft, for impacted persons. An SLA between Treasury and DOC governs management of the system, including appropriate use by DOC personnel, whereby all personnel granted system access are required to sign and abide by “Rules of Behavior” for appropriate system use. Additionally Cybersecurity and Privacy Awareness training is an annual requirement for all DOC employees, including those who maintain this system.

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.