Template Version Number: 01-2020

U.S. Department of Commerce
Office of the Secretary

Privacy Threshold Analysis
for the
Human Resources Management System (HR Connect)

U.S. Department of Commerce Privacy Threshold Analysis

Unique Project Identifier: [Number]

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a general description (in a way that a non-technical person can understand) of the information system that addresses the following elements:*
The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

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 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 purpose that the system is designed to serve*

HR Connect ensures 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.

e) *The way the system operates to achieve the purpose*

In 2010, DOC implemented a Human Resources Management System (HRMS) that complies with OPM's 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.

The Treasury HR Connect is a web-based enterprise solution built on PeopleSoft commercial- off-the- shelf (COTS) software. HR Connect transforms core back-office HR functions, moving them from a processing-centric capability supported by DOC, Bureau, and Operating Unit (OU) legacy systems, to a strategic-centric capability enabled through its commercial software underpinning. Additionally, self- service components of the software fundamentally transform the standard government HR service delivery model, putting additional information, services, and processes (i.e. personal data, position management, requests for personnel action, recruitment, reporting, etc.) directly in the hands of managers and employees.

From a business perspective, DOC's decision to migrate its HRSOs 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's 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.

f) A general description of the type of information collected, maintained, used, or disseminated by the system

PII is collected from DOC employees, managers, HR professionals and contractors and includes, but is not limited to1:

- Employee name and contact data (names, addresses, phone and email)
- Employee emergency contact data (names, addresses, phone and email)
- Citizenship, Race, and Ethnicity Data
- Disability Data
- Age
- Gender
- Banking (including bank account numbers and similar information used to support direct deposit of pay, and compensation data)
- Social Security number (to establish identity, as well as support compensation and payroll)
- Federal & State Tax Data
- Selective Service and Military Service Data
- Criminal and Debt History Data related to suitability for employment
- Education Data
- Beneficiary and Dependent Data (to include spouse information, children information)
- Health Benefit Data

g) Identify individuals who have access to information on the system

Access to HR Connect is limited to Department of the Treasury and DOC Employees and Managers, HR Connect System Administrators, Developers, and system maintenance personnel at the Federal Data Center located at the Memphis Computing Center.

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, Servicing HR Organizations (SHRO) 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

h) How information in the system is retrieved by the user

Data is retrievable by personal identifier. Data can be retrieved either by the employee identifier 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.

i) How information is transmitted to and from the system

Applicants who receive and accept job offers for employment with the DOC, submit information using a variety of forms which are required to complete the hiring/onboarding process – the PIA includes a comprehensive list of these forms, with hyperlinks where applicable.

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).

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.

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.

Questionnaire:

1. Status of the Information System

1a. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

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. *Continue to answer questions and complete certification.*

___ 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). *Continue to answer questions and complete certification.*

____ 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). *Skip questions and complete certification.*

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

____ Yes. This is a new information system.

____ Yes. This is an existing information system for which an amended contract is needed.

____ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

__X__ No. This is not a new information system.

2. Is the IT system or its information used to support any activity which may raise privacy concerns?
NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____ Yes. *(Check all that apply.)*

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

__X__ No.

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?
As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

___ Yes, the IT system collects, maintains, or disseminates BII.

__X_ No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

__X__ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

_X___ DOC employees
_X__ Contractors working on behalf of DOC
___ Other Federal Government personnel
____ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

__X__ Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, 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.
Provide the legal authority which permits the collection of SSNs, including truncated form. 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.

____ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

_X___ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?
Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

__X__ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

____ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the SAOP approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X__ I certify the criteria implied by one or more of the questions above **apply** to the Human Resources Management System (HR Connect)and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Information System Security Officer or System Owner Name: Kieu Lam Office: Deputy Director, HR IT, Enterprise Services Phone: 202-482-2899 Email: KLam@doc.gov Signature: KIEU LAM Digitally signed by KIEU LAM Date: 2020.12.10 11:56:31 -05'00' Date signed: _____	**Information Technology Security Officer** Name: Jerome Nash Office: IT Security Officer Phone: 202-482-5929 Email: jnash@doc.gov Signature: JEROME NASH Digitally signed by JEROME NASH Date: 2021.06.17 15:38:53 -05'00' Date signed: _____
Privacy Act Officer Name: Tahira Murphy Office: Office of Privacy and Open Government Phone: 202-482-8075 Email: TMurphy2@doc.gov Signature: TAHIRA MURPHY Digitally signed by TAHIRA MURPHY Date: 2021.08.09 12:52:23 -04'00' Date signed: _____	**Authorizing Official** Name: Rob Moffett Office: Acting IT Director, Enterprise Services Phone: 202-482-4644 Email: rmoffett@doc.gov Signature: ROBERT MOFFETT Digitally signed by ROBERT MOFFETT Date: 2020.12.10 12:13:22 -05'00' Date signed: _____
Bureau Chief Privacy Officer Name: Maria Dumas Office: Office of Privacy and Open Government Phone: 202-482-5153 Email: MDumas@doc.gov on behalf of: Signature: TAHIRA MURPHY Digitally signed by TAHIRA MURPHY Date: 2021.08.09 13:37:14 -04'00' Date signed: _____	