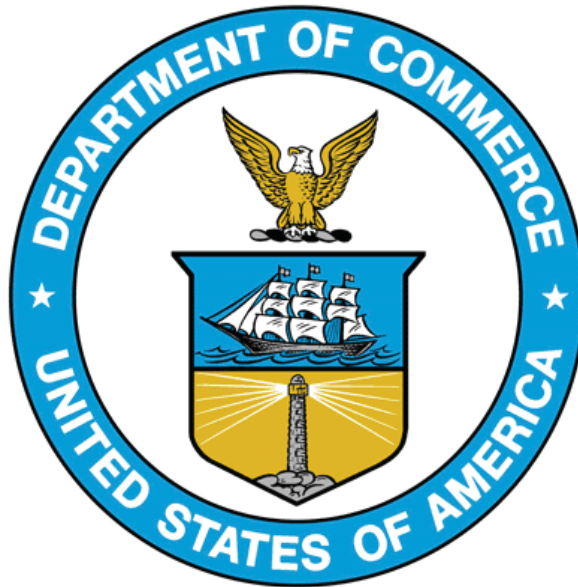


U.S. DEPARTMENT OF COMMERCE
Office of the Secretary



Privacy Threshold Analysis
for the Enterprise Services Human Resources Service System

U.S. Department of Commerce Privacy Threshold Analysis

Office of the Secretary/ Enterprise Services Human Resources Service System

Unique Project Identifier: OSE001 – Enterprise Services ServiceNow

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 on 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).

The DOC has developed this PTA to present existing and planned information for ensuring protecting this Moderate System in accordance with applicable laws.

The purpose of this PTA is to provide an overview of the security/privacy requirements of the Moderate System as well as to delineate the responsibilities and expected behavior of all individuals who access the system. The PTA shall be viewed as documentation of the structured process of planning adequate and cost-effective security/privacy protection for a system.

Description of the information system and its purpose

The Enterprise Services Human Resources Service System (HR ServiceNow) is a configured HR services information technology system that leverages ServiceNow, a cloud-based capability to provide case management and business process capabilities. DOC has configured HR ServiceNow to support critical human resources related mission functions on behalf of the Department.

In general, HR ServiceNow will allow authorized system users to submit, manage, and track human resources related requests including benefits, payroll requests, and Personnel Action Requests (PAR) of DOC employees. These requests and are referred to as “tickets.”

The new functionality for the HR ServiceNow system allows for the ability for authorized system users to upload supporting documentation and attach that documentation to HR related requests and for authorized, privileged users (Customer Service Representatives or CSRs) to make certain documentation, such as required notices (employee-obligor notifications) or submitted supporting documentation, available for viewing by authorized DOC users with a need to know via the HR ServiceNow Portal.

1. Notification of employee-obligor Functionality

For certain HR transactions that are processed, Federal laws and regulations require certain information or notices regarding the transaction be provided back to the requestor upon resolution.

HR ServiceNow allows authorized DOC users to log in to the system and see any tickets that either they opened, or that were opened on their behalf. The authorized DOC user is able to see the status of these requests, as well as any action that may need to be taken. In addition, federal notices for certain types of requests or transactions, such as garnishments, settlements, etc., will now be posted to the HR ServiceNow system and made available as an attachment to the ticket, viewable only by the designated, authenticated, and authorized DOC user and the CSR responsible for resolving the original request. Additionally, in some cases supporting documentation uploaded as part of the original request and attached to the ticket, may be made available for viewing by both the CSR resolving the ticket and the original requestor.

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

HR ServiceNow is a general support system for DOC Enterprise Services (ES) due to its necessity and use by all employees of the DOC. HR ServiceNow is a cloud-based computing software that provides the tools to request and support service requests for the business' customers. HR ServiceNow will be modified to allow ESHRSC processors to post employee-obligor notices to the HR Service Portal for authorized DOC users to view. Existing functionality to track requests related to Personnel Action Requests (PAR), Payroll, and Benefits will remain, as well as authorized DOC users ability to log into the system and see any tickets that either they opened, or that were opened on their behalf. The DOC user will be able to see the status of these tickets as well as any action that may need to be taken.

b) System location

ServiceNow Inc. has two datacenters that house redundant production instances of HR ServiceNow. One of them is in Culpeper, VA and the other is in Miami, FL. Table 1 provides more information regarding the data centers.

Table 1: ServiceNow Data Facilities

Location	Failover order
Miami, FL	Primary
Culpeper, VA	Standby

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

The HR ServiceNow system has the following interconnections:

HR Connect Imports

HR ServiceNow uses data from HRConnect to create HR service request records. The systems are not directly linked, but a data export is manually pulled from HRConnect and uploaded into HR ServiceNow. This upload creates new service request records in HRServiceNow, as well as updates existing service request records as needed.

HR ServiceNow also uses user data from HRConnect to augment DOC employee user records with information from HRConnect. Like the above import, ServiceNow and HRConnect are not directly linked, but a data export is manually pulled from HRConnect and uploaded into HR ServiceNow.

Enterprise Services Enabling Technology ServiceNow (ESET-SN) Interfaces

While PII and Business Identifiable Information (BII) is not shared with ESET-SN, the HR ServiceNow System has an interface with ESET-SN for service request information, along with user group data. ESET-SN, is another instance in ServiceNow owned by DOC.

Authorized DOC users will be able to open a ticket in either HR ServiceNow or ESET-SN. This requires an interconnection between the two systems to provide a seamless interface for the end user.

For non-service request tickets, the interconnection is bidirectional. All tickets that are created in HR ServiceNow are sent directly to ESET-SN. +Tickets created in ESET-SN are sent directly to HR ServiceNow if they are “human resources” related tickets. This interconnection takes place over secured protocols.

For Service Request tickets specifically, the interconnection is unidirectional. Service Request tickets, which can include either Payroll, Benefits, or PAR requests that are created in HR ServiceNow are sent directly to ESET-SN via secured protocols. ESET-SN and the HR ServiceNow system each have an authorized DOC user created within the other instance that grants their organization read privileges to specific modules.

Finally, the HR ServiceNow system sends User Group data in a unidirectional interconnection to ESET-SN. This data includes whether a user is designated as a Manager, and/or an HR Professional. The ESET-SN system uses this data to identify what types of HR services are displayed to the end user.

d) The purpose that the system is designed to serve

The HR ServiceNow system operates to improve the efficiency of HR functions at the DOC, including but not limited to, Personnel Action Requests, Incidents, Payroll and Benefits transactions. To accomplish this, PII/BII is collected, maintained, and processed by HR ServiceNow. This data is used in administrative matters, to improve Federal services online, for employee satisfaction, and for administering human resources programs.

e) The way the system operates to achieve the purpose

The HR ServiceNow system operates to improve the efficiency of HR functions at the DOC including but not limited to Personnel Action Requests, Incidents, Payroll and Benefits transactions. To accomplish this, PII/BII is collected, maintained, and processed in HR

ServiceNow. This data is used in administrative matters, to improve Federal services online, for employee satisfaction, and for administering human resources programs. Once the authorized DOC user has logged on and is authenticated to the system, the user will have access to the tickets that were created by them, as well as created on their behalf, any actions that they need to make, and federally required employee-obligor notices of transactions processed, or other supporting documentation (as necessary).

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

The HR ServiceNow system will collect and maintain Business Identifiable Information (BII) and/or Personally Identifiable Information (PII). This data is used in administrative matters, to improve Federal services online, for employee satisfaction, for administering human resources programs, and processing HR related transactions.

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

The HR ServiceNow system will be accessible to all authorized DOC users.

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

Authorized DOC users of HR ServiceNow can view the ticket number, status, and employee-obligor notices of their HR requests by accessing the HR Service Portal through the “Landing Page.” Additionally, user information can be retrieved by authorized privileged users of the system querying the application by ticket/transaction number, name or other pertinent data related to a specific ticket.

i) How information is transmitted to and from the system

Data is manually downloaded from HRConnect in order to support HR processing by the ESHRSC. This information is then uploaded to HR ServiceNow to create and update existing user records and tickets.

For Incident integration it is critical that for each HR ServiceNow Incident the ESHRSC staff know the key information (e.g. Incident Number and System Identification) for the corresponding ESET-SN Incident and vice versa. In a Unidirectional Integration, the DOC employee sends a request to the provider, either HR ServiceNow or ESET-SN, and the DOC employee must wait for the request to be carried out by the provider. The results are returned from the provider (e.g. Incident Number and System Identification) and the employee information (e.g. Incident) is updated on the employee’s end. For more information about the transmission of data between HR ServiceNow and ESET-SN ServiceNow, please refer to section 2c about the system interconnections.

Questionnaire:

1. 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	X
c. Significant System Management Changes	X	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. *Skip questions and complete certification.*

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

☒ 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 about: *(Check all that apply.)*

☒ Companies
☐ Other business entities

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

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: “The term ‘personally identifiable information’ refers to information which can be used to distinguish or trace an individual’s identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc...”

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

☒ DOC employees
☒ Contractors working on behalf of DOC
☒ 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 PII other than user ID?

☒ 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.

4c. 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.

☐ 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, and/or 4c are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the 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 HR ServiceNow Solution 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 HR ServiceNow Solution and as a consequence of this non-applicability, a PIA for this IT system is not necessary.


Name of Information System Security Officer (ISSO) or System Owner (SO): Nate Waugh

Signature of ISSO or SO: **NATHANIEL WAUGH**  Digitally signed by NATHANIEL WAUGH
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=NATHANIEL WAUGH, 0.9.2342.19200300.100.1.1=13001000451022
Date: 2018.08.13 13:29:07 -04'00' Date: _____

Name of Information Technology Security Officer (ITSO): Jun Kim

Signature of ITSO:  Digitally signed by JUN KIM
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=JUN KIM, 0.9.2342.19200300.100.1.1=13001001483988
Date: 2018.08.15 16:17:45 -04'00' Date: _____

Name of Authorizing Official (AO): Renee Macklin

Signature of AO: **RENEE MACKLIN**  Digitally signed by RENEE MACKLIN
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=RENEE MACKLIN, 0.9.2342.19200300.100.1.1=13001000231924
Date: 2018.08.16 15:51:07 -04'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): Wesley T Fravel

Signature of BCPO: **WESLEY FRAVEL**  Digitally signed by WESLEY FRAVEL
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=WESLEY FRAVEL, 0.9.2342.19200300.100.1.1=13001003618524
Date: 2018.08.13 11:52:27 -04'00' Date: _____