U.S. Department of Commerce
Office of the Secretary

Privacy Threshold Analysis
for the
Enterprise Services Human Resources Service System

High Privacy System/Moderate Security 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 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).

The Enterprise Services Human Resources Service System (HR ServiceNow and inContact) is a configured HR services information technology system that provides case management and business process capabilities for the Department of Commerce (DOC). Customer Service Representatives (CSR) use HR ServiceNow for HR case management, workflow, and incident management needs. CSRs use inContact as the telephony system for managing calls with customers.

The HR Service System supports critical DOC mission functions by acting as a tracker for all HR processing and Contact Center requests. The Enterprise Services Human Resources Service Centers (ESHRSC) use the HR Service System to manage HR related requests from creation to resolution. This requires the HR ServiceNow system to store and display relevant data to both process HR requests and solve HR problems, which will include PII for authorized DOC employees. Authorized DOC users supported by ESHRSC can not only create HR related tickets, but can authenticate into the HR Service Portal to see the status of their tickets and submit relevant HR documents required for processing.

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

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

1. **HRConnect imports**

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

2. **Enterprise Services Enabling Technology ServiceNow (ESET-SN) Interfaces**

While PII/BII information will not be shared with ESET-SN, the HR ServiceNow System will have an interface with ESET-SN for incident and service request information.

A user will be able to Ask a Question or open an incident 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 incident information, the interconnection is multidirectional. Incident tickets that are created in HR ServiceNow are sent directly to ESET-SN. Incident tickets created in ESET-SN are sent directly to HR ServiceNow. This interconnection takes place over secured protocols. For Service Requests, the interconnection is unidirectional. Service Request tickets, which can include either Payroll or Benefits requests that are created within HR ServiceNow are sent to ESET-SN via secured protocols.

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. In order to accomplish this, PII/BII is collected within HR ServiceNow. This data is used in administrative matters, to improve Federal services online, for employee satisfaction, and for administering human resources programs.

The inContact telephony system operates to manage and conduct all phone interactions with DOC employees or other end users.

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. In order to accomplish this, PII/BII is collected, maintained, or disseminated 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 HR Service Portal, the user will have access to the records 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.

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

The HR ServiceNow system collects 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.

The inContact telephony system will be modified to collect audio recordings from phone interactions. Any PII/BII will only be used by ESHRSC and will not be disseminated or stored past 90 days of use.

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

The HR ServiceNow system will be accessible to all authorized DOC users. Only ESHRSC employees who have been authorized to access inContact will be provided with the access to do so.

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. Additionally, user information can be retrieved by authorized privileged users of the system querying the application by ticket/transaction number.

Only ESHRSC employees who have been authorized to access inContact will be provided with the access to do so.

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 records.

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.*

__X__ 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): Collection of audio recordings (inContact)					

____ 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 01-2015). *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 01-2017 or later). *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.

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

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

____ No.

The inContact telephony system will be modified to collect audio recordings. Users of the telephony system will be informed that audio will be recorded for internal quality assurance and training purposes. Audio recordings will not be disseminated outside of ESHRSC or Enterprise Services, and only authorized employees will have access to the audio recording data.

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.)."

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

____ 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__ National Institute of Standards and Technology Associates
__X__ Contractors working on behalf of DOC
__X__ 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. SSNs are required for processing Human Resources transactions with various HR IT information systems within and outside of the Dept of Commerce.
Provide the legal authority which permits the collection of SSNs, including truncated form.

____ 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.

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

_X___ 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 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 Enterprise Services Human Resources Service System 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.

Name of Information System Security Officer (ISSO) : Nathaniel Waugh

Signature of ISSO : NATHANIEL WAUGH Digitally signed by NATHANIEL WAUGH Date: 2020.07.17 12:23:10 -04'00' Date: 07/17/20

Name of Information Technology Security Officer (ITSO): Jerome Nash

Signature of ITSO: JEROME NASH Digitally signed by JEROME NASH Date: 2020.07.19 16:16:03 -04'00' Date: 07/19/20

Name of Privacy Act Officer (PAO): Tahira Murphy

Signature of PAO: Tahira Murphy Digitally signed by Tahira Murphy Date: 2020.07.22 07:27:31 -04'00' Date: 7/22/2020

Name of Authorizing Official (AO): Robert Moffett

Signature of AO: ROBERT MOFFETT Digitally signed by ROBERT MOFFETT Date: 2020.07.17 15:02:00 -04'00' Date: ___________

Name of Bureau Chief Privacy Officer (BCPO): Maria Dumas

Signature of BCPO: MARIA STANTON-DUMAS Digitally signed by MARIA STANTON-DUMAS Date: 2020.07.21 14:55:34 -04'00' Date: 07/21/2020