Template Version Number: 01-2020

U.S. Department of Commerce
Office of the Secretary

Privacy Threshold Analysis
for the
Enterprise Services Enabling Technology ServiceNow (ESET-SN)
System

U.S. Department of Commerce Privacy Threshold Analysis

Office of the Secretary / Enterprise Services Enabling Technology ServiceNow (ESET-SN) System

Unique Project Identifier: OSES001

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this Information Technology (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).

This Privacy Threshold Analysis (PTA) applies to the Department of Commerce (DOC or "Department") Enterprise Services Enabling Technology ServiceNow (ESET-SN) System ("ESET-SN" and the NICE inContact CXone Customer Experience Platform"). The ESET-SN System leverages ServiceNow, a cloud-based capability that provides case management and business process capabilities and the NICE inContact CXone Customer Experience Platform which encompasses call recording for quality assurance and training purposes. DOC has configured ESET-SN to support critical human resources related mission functions on behalf of the Department.

In general, ESET-SN 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. Authorized users of ESET-SN (collectively, "authorized DOC users") include:

- DOC HR Service Center Customer Service Representatives ("Service Center CSR" or "CSR"), who use the System are generally made up of Contact Center representatives who intake and route inquiries, and DOC HR Specialists who analyze requests and provide HR services;
- DOC employees ("DOC employee users"), who use ESET-SN to submit HR related requests and related documentation, and to track the status of their requests, and

generally include both DOC employees with an HR inquiry, as well as personnel and supervisors within the DOC Office of Human Resources Management (OHRM);and

- ServiceNow system administrators ("administrators") who are responsible for administering the system.
- Regarding the NICE inContact CXone Customer Experience Platform, access will be limited to the Customer Service Representatives, select leadership personnel and key trainers.

These users may include contractors as well as Federal employees. Within these three user types, a subset of user groups ("sub-group") with specific permissions related to each module exist. Access to and permissions within the system are controlled at the sub-group level. For DOC employee users, default access is granted for the purposes outlined above (submitting and tracking their own tickets, etc.). For administrators and CSR users, system access is granted by filling out and submitting a user request form to the system administrator. This form includes a signature/approval of the user's supervisor and a selection of what sub-user groups the individual requires access to, in support of their duties. Once approved by the supervisor and system administrator, the individual is placed into the sub- groups for which they have been granted access and their permissions, including which modules and the permissions within each, are inherited from the sub-group. System modules are discussed in more detail below.

DOC employees can log into the system as described below and either initiate a new request or check on the status of current or previous requests, including those they opened as well as any that were opened on their behalf, any action that may need to be taken on their part, or any required employee- obligor notifications.

To accomplish this function, the ESET-SN system will collect, store, and process data relevant to HR request and actions, including Personally Identifiable Information (PII) on current and former DOC employees, as well as their dependents or beneficiaries.

The current services ESET-SN supports includes:

Service Center Incident Module or "Incident Module"

The primary function of ESET-SN is acting as a ticketing system for Service Center incidents and requests ("tickets"). The ESET-SN Service Center Incident Module (Incident Module) is used to manage the creation and tracking of such tickets. The Incident Module tracks each ticket from submission through resolution, and tracks communication between the Service Center CSR and the DOC employee. Tracking inquiry statuses and communication allows for detailed reporting about HR activity to DOC leadership.

This module may also be referred to as the "Incident Module."

Personnel Action Request (PAR) Module or "Service Requests Module"

The PAR Module tracks and reports on 'PAR Processing' for the DOC bureaus and agencies. DOC employee data collected includes employee identification and contact data including but not limited to name, business and personal email address, Notice of Action Code (NOAC), NOAC description, Veterans Identifier, and business and personal phone number. The ESET-SN PAR Module provides the following capabilities:

- □ Tracking a PAR transaction which includes ensuring all supporting documents are received
- □ Tracking PAR transactions processed in HRConnect
- □ Tracking synchronization errors associated with processing a PAR
- □ Tracking PAR documents archived with OPF/eOPF

Included in PAR tracking and management is the ability for select users (HR specialists and DOC Supervisors) to submit a PAR correction or update transaction, including any necessary supporting documentation. The PAR module may also be referred to as the "Service Requests Module."

Payroll and Benefits Module or "Service Catalog Module"

ESET-SN also provides service support for payroll and benefits tickets for DOC bureaus and agencies. Data collected includes DOC employee identification and contact data, including name, work location and address, business email address, NOAC, NOAC description, Veterans Identifier, business phone number, maiden name, and photocopies of drivers' licenses and passports.

The ESET-SN Payroll and Benefits Module provides the following:

Tracking a payroll and benefits transaction including ensuring all necessary supporting documentation is received

- □ Enhancing visibility to establish Department level metrics (i.e., dashboard)
- □ Enforcing standard transaction processing

Maintaining and improving transaction quality

This module may also be referred to as the "Service Catalog Module."

Landing Page Functionality or "Knowledge Module"

The Landing Page serves as the primary interface for authorized DOC users to find HR resources, create, submit, update, and track tickets, and initiate HR transactions.

DOC employee users use an online form available on the Landing Page, to submit tickets

that are worked by the Service Center CSRs. The Landing Page also consolidates bureau-specific HR information and DOC HR systems' hyperlinks for a "one-stop-shop" experience. Additionally, Knowledge Articles about Payroll, Benefits, PAR and other HR related items will be accessible from the Landing Page. Finally, the Landing Page displays events and reminders related to DOC Enterprise Service Shared Service Initiate Human Resources (SSI-HR) and communicates ESET-SN outages. This element of the landing page is also referred to as the "Knowledge Module."

The ESET-SN system imports the last name, first name, DOC email, Bureau, and DOC telephone number of DOC employees from Lightweight Directory Access Protocol (LDAP) into ESET-SN. This information is used to grant authorized DOC users access to ESET-SN through the Landing Page. ESET-SN inherits the authentication process implemented by the individual DOC Bureaus, ensuring the security of DOC employee profiles and information.

As outlined above, ESET-SN allows authorized DOC users to initiate a payroll, benefits, or PAR (update/correction only) transaction, in the form of a ticket, directly through the Landing Page. To process these requests, the DOC employee users may need to provide documentation which contains PII. For example, DOC employees wishing to change their enrollment and coverage status for DOC- provided health insurance from single to family may need to submit documentation demonstrating the change in their status – such as a birth certificate or marriage license. Such documentation will be attached to the ticket and stored encrypted within tables in ESET-SN. Required documents may be attached either by DOC employee users accessing the self-service requests on the Landing Page, or by Service Center CSRs creating service requests on behalf of an employee.

In addition to these modules, the system also includes a "Reporting Module" and a "Change Request Module." The Reporting Module allows for the creation, scheduling, editing, and sharing of reports generated using data from the other modules in the system, by a specific set of authorized users of the system. The Change Request module includes a capability to submit tickets to the DOC Change Control Board (CCB) to make changes to the ESET-SN system – for example adding a new workflow, creating a new user role, or adding a new field to an intake form.

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

ESET-SN is a major application for DOC Enterprise Services (ES) due to its necessity and use across the DOC.

b) System location

ServiceNow, Inc. is responsible for two datacenters that house redundant production instances of ESET-SN. One of them is in Culpeper, VA and the other is in Miami, FL. The Department of Commerce owns the data within the databases. 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 ESET-SN system has the following interconnections:

HR Connect Imports

ESET-SN 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 ESET-SN. This upload creates new service request records in ESET-SN as well as updates existing service request records as needed.

ESET-SN 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 ESET-SN.

d) The purpose that the system is designed to serve

The ESET-SN System provides a single point of entry to access ES offerings across the HR, Acquisition, IT, and Finance functional areas. The System will allow DOC users to view current ES announcements/notifications, get answers to common questions about ES services, submit requests for items or services, report errors, view status of cases, and find contact information for the ES Contact Center or area-specific points of contact.

e) The way the system operates to achieve the purpose

The ESET-SN instance provides a capability to request services for ES functional areas. The ESET-SN System has a knowledge base that provides information to DOC users, as well as links to all the modules they comprise. DOC users will have access to the cases that were created by the users, as well as those created on the users' behalf.

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

The ESET-SN System collects, maintains, or disseminates PII about DOC employees, contractors working on behalf of DOC, and other Federal Government personnel.

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

The ESET-SN System will be accessible to all authorized DOC users.

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

All authorized DOC users of ESET-SN can view the ticket number and status of requests relevant to them by accessing the ESET-SN web application.

Additionally, information can be retrieved by a limited set of privileged users of the system by querying the application by ticket number or any relevant data elements within the ticket (e.g. Employee Requested For, Opened By, etc.), through dynamic reporting/dashboarding (tickets assigned to the specific authorized DOC user logged in), or reports generated by the ESET-SN system. Privileged users include select members of the Enterprise Services HR Service Center, including CSRs, system administrators, and other authorized employees with a need-to-know such information.

i) How information is transmitted to and from the system

Data is manually downloaded from HRConnect to be uploaded to ESET-SN in order to create service requests (PAR tickets), and also to update or insert existing system user records.

Documentation for processing tickets can also be received through Accellion, a secure file transfer mailbox. When documentation is received through Accellion, it is never transmitted through an interface with ESET-SN. The documentation is verified outside of ESET-SN and then attached to the ESET-SN ticket. For some transactions, such as PAR updates or corrections, ES has instructed end users to use a dedicated form in the portal, rather than Accellion, to initiate such a ticket.

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 completecertification.*

___ 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 or 01-2017). *Continue to answer questions and complete certification.*

__X__ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (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.

____ 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): HR incident tracking			

___ 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.
____ 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."

____ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that*

apply.)

___ DOC employees
___ 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?

___ Yes, the IT system collects, maintains, or disseminates SSNs, includingtruncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.
Provide the legal authority which permits the collection of SSNs, including truncated form. (HR director to provide)

____ 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?

___ 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.

___ 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 Enterprise Services Enabling Technology ServiceNow (ESET-SN) 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.

Information System Security Officer or System Owner Name: Nathaniel Waugh Office: ISSO Phone: 202-482-1540 Email: NWaugh@DOC.gov Signature: NATHANIEL WAUGH Digitally signed by NATHANIEL WAUGH Date: 2021.01.27 08:35:03 -05'00' Date signed: 1/27/21	**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: 2021.01.28 13:53:57 -05'00' Date signed: 1/27/21
Privacy Act Officer Name: Lisa J. Martin Office: Office of Privacy and Open Government Phone: 202-482-2459 Email: Lmartin1@doc.gov Signature: LISA MARTIN Digitally signed by LISA MARTIN Date: 2021.02.18 11:00:33 -05'00' Date signed: 02/18/2021	**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: 2021.01.28 13:29:54 -05'00' Date signed: 1/28/21
Bureau Chief Privacy Officer Name: Maria Dumas Office: Office of Privacy and Open Government Phone: 202-482-5153 Email: MDumas@doc.gov Signature: MARIA STANTON-DUMAS Digitally signed by MARIA STANTON-DUMAS Date: 2021.02.22 10:37:26 -05'00' Date signed:	