Version Number: 01-2019

U.S. Department of Commerce
Office of the Secretary

Privacy Impact Assessment
for the
Enterprise Services Enabling Technology ServiceNow System

Reviewed by: Maria 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 02/22/2021

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

U.S. Department of Commerce Privacy Impact Assessment
Enterprise Services Enabling Technology ServiceNow (ESET-SN) System

Unique Project Identifier: OSE001 – Enterprise Services Enabling Technology ServiceNow (ESET-SN) System

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.

This Privacy Impact Assessment (PIA) applies to the Department of Commerce (DOC or "Department") Enterprise Services Enabling Technology ServiceNow (ESET-SN) System 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 HR case management, workflow, and incident management needs, and 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, and a more detailed description of the user groups and their permissions within each module is included in Section 6.3.

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. A further discussion of the types of PII collected and used for each system function can be found below and in Section 2 of this PIA.

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 HR 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 ofsystem

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 HRServiceNow, 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 way the system operates to achieve the purpose(s) identified in Section 4

ESET-SN operates to improve the efficiency of HR functions at the DOC, including but not limited to, Personnel Action Requests, Payroll and Benefits transactions, and resolving questions and incidents on behalf of DOC employees. To accomplish this, PII/BII is collected, maintained, and processed in ESET-SN. This data is used in administrative matters, to improve Federal services online, for employee satisfaction, and for administering human resources programs. BII collected is inclusive of DOC Bureau, NOAC, NFC, and HR Connect information, and DOC insurance and financial providers.

Section 4: Purpose of the System further discusses the way the system operates to achieve the purpose.

(e) 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 HR 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.

(f) 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, too initiate such a ticket.

(g) Any information sharing conducted by the system

Information is shared via the interfaces ESET-SN utilizes. All user information is restricted to DOC authorized users only.

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

Specific programmatic authorities include the following, with all revisions and amendments: 5 U.S.C., Title 31 U.S.C. 66a, 492, Title 44 U.S.C. 3101, 3309, 5 U.S.C. 301; 44 U.S.C. 3101; Executive Office (E.O.) 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 1987. The authority to deliver, maintain, and approve department-wide and bureau-specific automated human resources systems and serve as the focal point for the collection and reporting of human resources information within the Department of Commerce (DOC) is delegated to the Office of Human Resources Management (OHRM). This authority is identified by Departmental Organization Order (DOO) -- 20-8 - SECTION 4.

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

Moderate

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):					

_ 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 01-2015).

_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 01-2017 or later).

Section 2: Information in the ESET-SN 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	X	j. Financial Account	X
b. Taxpayer ID	X	g. Passport	X	k. Financial Transaction	
c. Employer ID	X	h. Alien Registration	X	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 need to collect, maintain, or disseminate the Social Security number, including truncated form: Solicitation of the SSN is authorized as per Executive Order 9397 of November 22, 1943, as amended by Executive Order 13748 (https://www.gpo.gov/fdsys/granule/CFR-2009-title3-vol1/CFR-2009-title3-vol1-eo13478/content-detail.html). The purpose is to provide the SSN as the means of unique identification to facilitate accurate HR processing and reporting for the Department of Commerce. Social Security numbers are not a defined field that is explicitly maintained or requested by the system but may be collected as part of supporting documentation needed to process an HR request, and maintained as unstructured data. **Information may include photocopies of such documents or similar identity-establishing documents, used as supporting documentation for an HR request, and are maintained as unstructured data in the system.					

General Personal Data (GPD)					
a. Name	X	h. Date of Birth	X	o. Financial Information	X
b. Maiden Name	X	i. Place of Birth	X	p. Medical Information	X
c. Alias	X	j. Home Address	X	q. Military Service	X
d. Gender	X	k. Telephone Number	X	r. Criminal Record	X
e. Age	X	l. Email Address	X	s. Physical Characteristics	X
f. Race/Ethnicity	X	m. Education	X	t. Mother's Maiden Name	X
g. Citizenship	X	n. Religion	X		
u. Other general personal data (specify): * - Limited medical information may be contained in insurance documentation for new hires. Likewise, physical characteristics may be captured in supporting documentation associated with a specific HR request. Such data is maintained as unstructured data in system.					

Work-Related Data (WRD)					
a. Occupation	X	e. Work Email Address	X	i. Business Associates	X
b. Job Title	X	f. Salary	X	j. Proprietary or Business	

				Information	
c. Work Address	X	g. Work History	X		
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information			
k. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	X
b. IP Address	X	d. Queries Run	X	f. Contents of Files	X
g. Other system administration/audit data (specify):					

Other Information (specify)
Reports are generated by system queries on HR transactions and requests in assistance for process improvement.

2.2 Indicate sources of the PII/BII in the ESET-SN system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person		Hard Copy: Mail/Fax	X	Online	X
Telephone	X	Email	X		
Other (specify): Voicemail with name and business telephone for call back (Voicemails are purged from the system after they are listened to each day). Emails that contain PII must provide access to this data using DOC secure Accellion file transfer service or uploaded directly in ESET-SN by either the DOC employee user, or a CSR or other privileged user opening a ticket on behalf of a DOC employee. Voice recordings are retained on the NICE inContact Platform for a period of 90 days and then automatically deleted.					

Government Sources					
Within the Bureau	X	Other DOC Bureaus	X	Other Federal Agencies	X
State, Local, Tribal		Foreign			
Other (specify): A query is pulled from HRConnect and manually uploaded to ESET-SN. This query contains PAR transaction information including but not limited to name, email address, Notice of Action Code (NOAC), NOAC description, Veterans Identifier, and a phone number. To process HR transaction requests, worklist queries are extracted from DOC HR systems via a secure HTTPS connection and saved as a spreadsheet on a GFE laptop. This data is uploaded into ESET-SN via a secure HTTPS connection to manually import the saved file into the appropriate Module.					

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.

Ensuring the accuracy of information in the ESET-SN system is a shared responsibility amongst authorized DOC users of the system. DOC employee users are responsible for checking their own information, including contact information and information submitted as part of a HR service request or ticket, for accuracy. Per DOC policy, DOC employee users must ensure the information provided is accurate prior to adding documentation to a ticket that is created through self-service means (i.e. submitting a ticket through the Landing Page). For ESET-SN tickets that are initiated by an authorized privileged user (a Service Center CSR), it is the responsibility of the privileged user to verify that the information provided in documentation being attached is accurate and relevant to the authorized DOC user for whom the ticket has been created.

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. ESET-SN is used for resolving HR related issues through HR Service Now is generally repurposed or previously collected through source systems. Information collections (and OMB control numbers) are specific to the form being used to collect source information at the original point of collection.
	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	X	Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

	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 ESET-SN 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	X	For employee or customer satisfaction	X
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).

ESET-SN will support ES DOC's HR mission and vision to provide innovative, data- driven, and customer-centric services that enable DOC employees to carry out the department's mission objectives.

The PII collected is for the purpose of supporting and tracking Human Resources actions, requests or questions. The information is used by the following:

- ESET-SN to respond to customer inquiries and requests.
- HR PAR Processors, as well as Payroll and Benefits Processers, for tracking and processing PAR, or Payroll and Benefits related actions and requests.
- Reporting for DOC Enterprise Services organization for status and process improvements.

The purpose of the collection of this information includes providing the following data:

- Workflows and process management based on the organization needs
- Knowledge repository for all HR content
- Managed content display based on the organization's HR lifecycle
- Insight into vendor managed transactions
- HR Transaction Information

The information used and collected by the information system is to track the lifecycle of PAR, Payroll and Benefits request, as well as provide processing request/incident status to customers. In order to process PAR, Payroll, and Benefits requests, ESET-SN must collect the PII of federal employees. In some cases, such as when beneficiary information is needed for the request, information from members of the public may be collected. Data may be collected for former/separated/retired employees depending on the approved scope and Standard Operating Procedure (SOP) for any given type of service, including Incidents, PAR, Payroll, Benefits.

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.)

The potential privacy threats to ESET-SN personnel and Commerce employees include:

- Physical damage to a data facility – Fire, Water, Hurricane
- Compromise of Information – eavesdropping, theft of media, retrieval of discarded materials, inadvertent disclosure of user information to incorrect user
- Technical Failures – hardware, software
- Compromise of Functions – error in use, abuse of rights, denial of actions
- Lack of data minimization (more information than is necessary is collected)
- Risks of accuracy, relevance, and completeness of information in the system
- Risks to consent as users have their information automatically uploaded into the system, and may need to submit other data in order to have their issue(s) resolved

The operating unit has implemented all required NIST security controls for a moderate system and all DOC required Privacy controls for a high privacy system to ensure the safety of information is retained by handling, retaining, and disposing of appropriately. These controls include, but are not limited to, access control, role-based access management, authorization, audit and accountability, configuration management, identification and authentication, and encryption. DOC policy and procedure governs appropriate use of the system 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 privileged basis.

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	
DOC bureaus	X	X	
Federal agencies			
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.

Electronic documents received through ESET-SN will not be shared with any other system.

6.2 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: see below.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

This IT system manually receives information from another IT system(s) that is (are) authorized to process PII. A query of all DOC employees will be manually pulled from the HRConnect system and will be sent to ESET-SN via a secure file transfer method once per Pay Period (every two weeks). The data HRConnect will provide includes but is not limited to first name, last name, middle name, office, Bureau, work email, and title. The ESET-SN system is not responsible for maintaining employee data within the HRConnect system (i.e. active vs. former employees).

PAR tracking data from the Entry on Duty (EOD) list provided by the DOC Bureaus and a query pulled from HR Connect is manually uploaded into ESET-SN. Only authorized personnel are able to work with this data. The data that is imported includes and is not limited to employee name, Bureau, Office, Veterans Identifier, Point of Contact information, Name, Employee ID, Email, Office Bureau, NOAC, EOD/Eff Date, Initiator, Employee Record, Effective Sequence, Status of Records, and SINQ codes. The data is used in the PAR Module. The DOC Bureaus use Accellion to provide ESET-SN with initial PAR tracking data from EOD lists and PAR transactions to be processed. Any PAR updates or changes after initial ticket creation must use the dedicated PAR correction intake form in the portal.The PAR Module is also built with a capability to generate automated emails to notify specific DOC POC's for the PAR transactions referenced, using ESET-SN and DOC email system using all proper FIPS 140-2 crypto module regulations at various stages of PAR processing (e.g. missing documentation, action successfully applied at NFC etc.).

Payroll and Benefits transactions will be tracked in ESET-SN. As Payroll and Benefit transactions are sometimes PAR transactions, the information will be pulled from HR Connect as described previously. Additionally, authorized DOC users will have the ability to submit documentation directly into ESET-SN. These documents will contain PII directly referenced in this document.

6.3 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): Authorized DOC HR Contractor staff. See description of user groups, modules, and related permissions outlined in the table below.			

	GENERAL USER TYPES	
	DOC EMPLOYEE USERS	
ID	Sub-User Group	Primary Use of the System
DEU-1	DOC Employee Users	Employee users within the DOC who submit HR related tickets and similar requests through ESET-SN.
DEU-2	DOC Local HR	HR Personnel assigned to specific Bureaus enterprise-wide
DEU-3	DOC Managers	HR Personnel who oversee OHRM function at DOC
	HR SERVICENOW ADMINISTRATORS	
ADM-1	LDAP Admin	Oversee DOC LDAP which is used to facilitate permissioning in the system
ADM-2	User Management Admin	Oversee creation and management of landing page content.
ADM-3	System and Security Group	Oversee management of system, including granting system access, assigning sub-groups for users, and monitoring system use.
ADM-4	Knowledge Admin	Oversee management of knowledge module, including content developed and deployed.
	SERVICE CENTER CSRS	
CSR-1	Contact Center Tier 1	Intake and respond to basic HR and PAR inquiries and route to Tier 2 as necessary
CSR-2	Contact Center Tier 2*	Processing of PAR, compensation, classification, staffing, and benefits tickets, including intake of escalated tickets from Tier 1
CSR-3	Contact Center Tier 3**	Intake and routing of IT-related inquiries associated with ESET-SN
CSR-4	Benefits Quality Analysts	Create, update, approve, and manage catalog of knowledge materials and intake mechanisms for benefits related service catalog
CSR-5	Benefits Managers	Oversee benefits specialists
CSR-6	Benefits Specialists	Resolve benefits related issues, process HR services for benefits related requests
CSR-7	Compensation Quality Analysts	Create, update, approve, and manage catalog of knowledge materials and intake mechanisms for compensation related service catalog
CSR-8	Compensation Managers	Oversee compensations specialists
CSR-9	Compensation Specialists	Resolve compensation related issues, process HR services for compensation related requests
CSR-10	Special Handling Assistants	Facilitate resolution of unique or specific HR-related issues that cannot be resolved by Tier 1 or 2 CSRs or by benefits, compensation, or PAR specialists or managers.
CSR-11	Special Handling Managers	Oversee Special Handling group
CSR-12	Document Control	Handle intake of HR documentation/documents associated with a PAR
CSR-13	Document Control Managers	Oversee document control group
CSR-14	PAR Import	Import Personnel Action Requests (PAR) from HRConnect to ESET-SN
CSR-15	PAR Managers	Oversee Personnel Action Request (PAR) Processing team/PAR specialists
CSR-16	PAR Processing	Resolve Personnel Action Requests (PAR) related issues, process PARs
CSR-17	PAR Viewers	Contact Center Users (Tier 1 & 2) Authorized to view PARs to respond to specific inquiries.
CSR-18	Reporting Managers	Oversee reporting functionality and service management
CSR-19	Service Management	Oversee creation, editing, and sharing of reports generated from information in the system.

*Contact Center Tier 2 sub-user groups are further broken down into specific areas: Payroll, PAR Processing, Staffing, and Classification, with each sub-user group responsible for triaging tickets specific to those areas.

**Contact Center Tier 3 sub-user groups are broken into 2 specific areas: DOC Enterprise Services and Treasury HR Connect, with each sub-user group responsible for triaging tickets specific to those areas.

MODULE & PERMISSION		DEU			ADM				CSR																			
		1	2	3	1	2	3	4	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
Service Center Incident (Incidents)	Create	X	X	X			X	X	X	X	X									X	X						
	Update						X	X	X	X	X									X	X						
	Close						X	X	X	X	X									X	X						
	View	X	X	X			X	X	X	X	X									X	X						X
PAR (Service Requests)	Create						X						X	X		X	X			X	X		X	X			
	Update						X						X	X		X	X			X	X		X	X			
	View						X		X				X	X		X	X			X	X		X	X	X		X
	Approve						X							X			X				X		X	X			
	Close						X														X		X				
Payroll & Benefits (Service Catalog)	View (Settlements)																	X	X								
	Edit (Settlements)																	X	X								
	View (Garnishments)															X	X	X	X								
	Edit (Garnishments															X	X	X	X								
	Create	X	X	X								X	X	X	X	X	X			X	X		X	X			
	Update											X	X	X	X	X	X			X	X		X	X			
	View	X	X	X								X	X	X	X	X	X			X	X		X	X			X
	Approve											X	X		X	X											
	Delete																										
Knowledge (Landing Page)	Create					X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Update					X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Approve					X	X																				
	Archive						X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Delete						X																				
Change Requests	Create						X	X	X	X	X									X	X						
	Update						X	X	X	X	X									X	X						
	Close						X	X	X	X	X									X	X						
	View						X	X	X	X	X									X	X						
Reporting	Create						X	X	X	X	X										X		X	X		X	X
	Share						X	X	X	X	X										X		X	X		X	X
	Edit						X														X		X			X	X
	Schedule						X														X		X			X	X
	Delete						X														X		X			X	X
	View Metric Instance						X														X		X			X	X

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: . ESET-SN is used for resolving HR related issues through ESET-SN is generally repurposed or previously collected through source systems. As such, Privacy Act Statements are provided to users at the original point of collection for this information. Additionally, language is provided on the landing page and at the bottom of each page where users may submit a ticket.	
X	Yes, notice is provided by other means.	Specify how: All outbound emails sent by the ESET-SN system contain standard footer text highlighting that PII is being collected and used at https://enterpriseservices.servicenowservices.com/es?id=es_privacy_policy Additionally, users are advised of the collection and use of their information via a security warning banner and a privacy notice available at https://commerceenterpriseservices.servicenowservices.com/hr?id=privacy
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII or decline consent to be recorded.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Individuals may decline to provide PII/BII which may result in the denial or refusal of a benefit and ultimately the failed processing of a financial transaction (e.g., payment, reimbursement). Callers refusing to be recorded can be provided the option to submit an email inquiry as an alternative method for assistance.
	No, individuals do not have an opportunity to decline to provide PII/BII.	

7.3 Indicate whether and how individuals have an opportunity to consent to particularuses 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: PII collected is limited to the minimum amount required on a form for a specific transaction. Individuals do not have an opportunity to consent to particular uses of their PII/BII as failure to provide the necessary information will prevent processing of the request.

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: Individuals can contact HR and update relevant information maintained in the system via email, phone, submitting new documentation, or by creating a new service request or ticket to update their information.
	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.)*

X	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: Access to files or electronic media is restricted to authorized DOC employees or contractors only. Access logs are also kept and reviewed for any anomalies.
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): March 26, 2020 ☐ 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	Voice recordings are stored on a secured S3 infrastructure using AES-256 encryption at rest and TLS1.2 in transit. The voice recordings are saved for a period of 90 days and then automatically deleted.

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).*

The PII/BII data used in the ESET-SN system is transferred in a secure fashion and unauthorized use of the data is restricted by user authentication and access management.

Information in transit and at rest is encrypted using FIPS 140-2 validated encryption modules, which are described in further detail below:

- ServiceNow, Inc. uses self-encrypting hard drives for database servers, which leverage a FIPS 140-2 Level 2 validated encryption module (Cert# 1635).
- ServiceNow Inc. uses Transport Layer Security (TLS) 1.2, Advanced Encryption Standard (AES) with 256-bit encryption (High)
- DOC's Accellion Secure file transfer is used to transfer data and end user documentation to authorized DOC POC's and contractor personnel from DOC Bureaus. Accellion uses TLS 1.2 AES with 128-bit encryption (High); ECDH with 256 bit exchange to ensure data is secure in transit.
- Sensitive data contained in reports is encrypted using FIPS 140-2 validated cryptographic modules.
- All government representatives (employees and contractors) are issued DOC Government Furnished Equipment (GFE) Laptops running a secure government approved baseline that encrypts all data at rest using a FIPS 140-2 validated cryptographic module.

ESET-SN has also implemented the following measures to protect PII and BII in the system:

- Accounts on Lightweight Directory Access Protocol (LDAP) enabled hosts enforce approved authorizations for access in accordance with the account maintained in the LDAP repository. All accounts on non- LDAP-enabled hosts enforce approved authorizations access in accordance with the accounts maintained locally.
- For authorized privileged users (i.e. CSRs, system administrators, etc.), ESET-SN uses its own Role Based Access Control (RBAC) model, aswell as implemented two factor authentication.
- Using RBAC, the ESET-SN system prevents individuals from seeing information that does not result from a business need.
- Additional security measures include implemented whitelisting, which is the ability to restrict ESET-SN access to the system over authorized and trusted DOC networks.
- Authorized DOC users are managed via the DOC Bureaus. Every government representative goes through a background check from the DOC before being granted access to a PIV card and GFE. Each representative is then only given access to the ServiceNow data that is needed to perform their job after security and privacy training is completed.
- Access logs are kept and reviewed for any anomalies.

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/Department 18 - Employee Personnel Files Not Covered By Other Agencies
	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: The retention period for these records is guided by the General Records Schedules (GRS), which are issued by the National Archives and Records Administration (NARA) to provide disposition authorization for records common to several or all agencies of the Federal Government. In accordance with GRS 20, item 3, electronic versions of records scheduled for disposal may be deleted at the expiration of the retention period authorized by the GRS for the equivalent paper copies or when no longer needed, whicheveris later. Various items in GRS 1, Civilian Personnel Records, authorize the disposition of the records described in this PIA.
	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	
Degaussing		Deleting	
Other (specify):			

**In the event that paper copies are received, the ESET-SN system will shred the documents after scanning them.*

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 levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: PII on HR documentation can be used to identify individuals. Name information, Nature of Action Code, veteran identifier, and work-related data (WRD – refer to table 2.1), General Personnel Data (GPD – Refer table 2.1), Identifying numbers (IN – Refer table 2.1) is displayed as part of the process and securely archived with in the information System.
X	Quantity of PII	Provide explanation: The ESET-SN system will hold information about all DOC employees as well as any listed beneficiaries and/or dependents.
X	Data Field Sensitivity	Provide explanation: PII on HR documentation can be used to identify individuals and may include sensitive data such as copies of driver's licenses and other identity documents, Social Security numbers, etc. Name information, Nature of action, veteran identifier, and work-related data (WRD – refer to table 2.1), General Personnel Data (GPD – Refer table 2.1), Identifying numbers (IN – Refer table 2.1) is displayed as part of the process and securely archived with in the information System.
X	Context of Use	Provide explanation: ESET-SN is used in processing HR transactions, which includes making determinations about individuals benefits.

X	Obligation to Protect Confidentiality	Provide explanation: Information maintained in the system includes that which is subject to the Privacy Act. Additionally, based on the system's FIPS 199 security categorization, the management, operational and technical security controls required for the System (ACI) Tracking Solution at a minimum, include all Moderate baseline security controls documented in NIST SP 800-53, Rev. 4. New security measurements for the information system were developed to enhance the FedRAMP moderate baseline security controls and additional FedRAMP guidance and requirements. The
		FedRAMP moderate baseline security controls extend the NIST SP 800-53, Rev. 4 moderate baseline controls are needed for the assurance of government data in cloud products and services. The security information was added to provide the additional confidentiality to the PAR tracker system of the information system.
X	Access to and Location of PII	Provide explanation: Access to PII is limited to authorized DOC personnel only and in a secure space. PII will be located in within an access controlled secure space.
	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.)

The potential privacy threats to ESET-SN personnel and Commerce employees include::

- Compromise of Information – eavesdropping, theft of media, retrieval ofdiscarded materials, risks of inadvertent disclosure of user data
- Technical Failures – hardware, software
- Compromise of Functions – error in use, abuse of rights, denial of actions

ESET-SN has implemented security controls required by DOC policy and recommended by NIST SP 800-53, Rev. 4 to ensure the safety of information. For example, access control, audit and accountability, configuration management, identification and authentication controls are implemented.

ESET-SN use's multiple security appliances and tools (ex. Firewall, IDS/IPS, Anti- malware) to protect the privacy of the information. Certain networks are whitelisted so that employees can only access ServiceNow from approved networks or through a VPN. This will protect the privacy of individuals on unsecure networks.

Additionally, use of the system is governed by DOC policy and procedure, and users receive annual training on privacy and information security awareness.

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.