Version Number: 01-2015

U.S. Department of Commerce
Office of the Secretary

Privacy Impact Assessment
for the
HR Now

Reviewed by: Michael Toland, 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

Catrina D. Purvis

Digitally signed by Catrina D. Purvis
DN: cn=Catrina D. Purvis, o=Office of the Secretary, Office of Privacy and Open Government, ou=US Department of Commerce, email=cpurvis@doc.gov, c=US
Date: 2016.12.21 11:08:02 -05'00'

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

U.S. Department of Commerce Privacy Impact Assessment
Office of the Secretary
HR Now

Unique Project Identifier: OSES001 - Enterprise Services ServiceNow

Introduction: System Description

Provide a description of the system that addresses the following elements:

(a) a general description of the information in the system

Employee data includes employee identification and contact data such as name, email address, and a phone number where they can be reached. This information is required to enable HR NOW Agency Designees to document and track support requests.

The system utilizes the FedRAMP Moderate ServiceNow Service Automation Government Cloud Suite to provide an incident and user support ticketing system.

Access to HR Now is via DOC Trusted Internet Connection and restricted to authorized DOC users on DOC networks.

HR Now provides the following functions:

- Report Issues and Ask Questions
- Access HR Rules and Regulations
- Communicate with HR Service Center staff

The boundary of the system will include several automated layers (Customer Experience, Service Management, Enterprise Solution and Reporting & Analytics Layer) as part of the supported system boundary of the information system. All these layers are part of the Service Management Solution Conceptual Model for the system.

(b) a description of a typical transaction conducted on the system

HR System Incident Report

- User experiences an incident utilizing a separate supported HR system.
- User submits an incident report via
  - Directly inputs incident via self-service HR Now web page
  - Telephones the Contact Center to allow the Tier 1 Customer Service Representative to enter the incident record. This can occur by direct telephone communication, or by leaving a voice mail after operating hours, which may or may not require a call-back for clarification.
- Tier 1 CSR reviews request and responds with solution by phone or email, or
- Tier 1 escalates complex requests to Tier 2 for resolution.
- Tier 2 resolves incident and notifies requestor of resolution by phone or email.

HR System Help Request

- User requires functional assistance with system navigation for a supported HR System
- User submits a Help Request via
  - Directly inputs request via self-service HR Now web page
  - Telephones the Contact Center to allow the Tier 1 Customer Service Representative to enter the help request. This can occur by direct telephone communication, or by leaving a voice mail after operating hours, which may or may not require a call-back for clarification.
- Tier 1 reviews request and responds with solution by phone or email, or
- Tier 1 escalates complex requests to Tier 2 for resolution.
- Tier 2 resolves incident and notifies requestor of resolution by phone or email.

(c) any information sharing conducted by the system

The information provided by the System is used only for authorized activities performed by internal personnel only. Information sharing by the system will be limited to a case by case basis. While information will not be shared with other systems in an ongoing fashion, it will have the capability to produce reports on incidents and requests. The use of such information sharing would be to inform the business areas where they are originating to inform process improvement (i.e. minimizing the occurrence of common issues). Such reports will not include information about individuals who request information.

(d) a citation of the legal authority to collect PII and/or BII

Includes the following, with all revisions and amendments: 5 U.S.C. 301; 44 U.S.C. 3101; 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.

The PII and BII data is collected by the system to enable identification of the HR data and facilitate the existing HR System Account Requests application process. It is provided to the interface system so that classification activities can be performed on the HR System Account Request process application system.

(e) the Federal Information Processing Standard (FIPS) 199 security impact category for the system

The *potential impact* is MODERATE based on (FIPS) 199

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

_X_ 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):					

Section 2: Information in the 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*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport		k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
b User ID (Derived from email address)					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address		o. Medical Information	
d. Gender		j. Telephone Number	X	p. Military Service	
e. Age		k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation		d. Telephone Number	X	g. Salary	
b. Job Title	X	e. Email Address	X	h. Work History	
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify): Bureau, Department, Office					

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): N/A					

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

Other Information (specify)

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

Directly from Individual about Whom the Information Pertains					
In Person		Hard Copy: Mail/Fax		Online	X
Telephone	X	Email	X		
Other (specify): Voice Mail with name and business telephone for call back.					

Government Sources					
Within the Bureau	X	Other DOC Bureaus	X	Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify): A personnel directory will come from within the DOC and other DOC bureaus in the form of an extract file which will be manually entered into the HR Now system.					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify): N/A					

2.3 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		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

X	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 IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
To determine eligibility		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).

When Collected the PII will be used for the purpose of administering human resources programs.
Some of the purposes of the collection of this information is to provide the following data:

- Workflow and process management based on the organization needs.
- Links to training guides.
- Managed content display based on the organization's HR lifecycle
- Insight into vendor managed transactions
- Single source of truth

All the information used and collected by the information system is only related to the name and email of a federal employee/contractor and it is used for the general administration of human resource programs.

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		
DOC bureaus	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.

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: The system imports personnel directory data from NFC. The import file from NFC is encrypted at rest and in transit
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

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):			

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 other means.	**Specify how:** Yes, the notice is accessible from a "Policy and Security" link provided on the HR Now Portal Home Page https://commerceenterpriseservices.service-now.com/HRNow **"**Thank you for visiting the U.S. Department of Commerce HR Now website and reviewing our privacy policies. Personally identifiable information you provide will be used in connection with the Department of Commerce's HR Now System to respond to Human Resources system support questions, incident tracking, and change requests. The data residing in the application and the data you provide carries the designation of Sensitive-but-Unclassified or SBU data and is protected under the Privacy Act. The information we collect may be used for such other purposes as are described in the Privacy Act System of Record Notice entitled " Commerce Dept-18, Employee Personnel Files Not Covered by Notices of Other Agencies" The information we have about you may also be disclosed to other Federal, state and local agencies for law enforcement or other lawful purposes as permitted by the Privacy Act. Providing the requested information is voluntary. However inquiries and requests cannot be processed without the correct information. In order to maintain the highest level of customer confidence, we track and record information about our customers and their web activities to ensure security and privacy. We collect personally identifying information (name, email address, phone number) if specifically and knowingly volunteered by you. We are committed to protecting our customer's privacy through the adoption of the federal privacy principles. For more detailed information use the hyperlink below to view the Privacy Act of 1974." **During onboarding, employees will receive notice and must consent to:** Personnel data is classified as "sensitive but unclassified" (SBU). "Sensitive" data is defined as any information that the loss, misuse, or unauthorized access to - or modification of - could adversely affect the national interest, the conduct of Federal Programs, or the ***privacy to which individuals are entitled under section 552a of Title 5, USC (The Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or Act of Congress to be kept secret in the interest of national defense or foreign policy.*** Unauthorized access, manipulation or disclosure of sensitive personnel data is deemed to invade the privacy to which individuals are entitled under the Privacy Act.
	No, notice is not provided.	**Specify why not:**

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

X	Yes, individuals have an opportunity to decline to provide PII/BII.	**Specify how:** With the exception of Personnel Directory Information imported from NFC, the user can decline to provide PII (e.g., personal phone number to receive a call back).
	No, individuals do not have an opportunity to decline to provide PII/BII.	**Specify why not:**

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses 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:** Individuals are not given an opportunity to give consent after the initial Human Resources hiring process. The accounts are established at inception via Personnel Directory Information imported from NFC.

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:** Employees have the opportunity to review/update their personnel directory information using the NFC Employee Personal Page (EPP).
	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: All access is recorded by the system as well as the input/output related to all entries in the system. The data is archived for forensic purposes.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): _____ [X] 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 (POAM).
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 ownership rights over data including PII/BII.
X	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

Accounts on LDAP-enabled hosts enforce approved authorizations for logical access in accordance with the account privileges maintained in the LDAP repository. All accounts on non-LDAP-enabled hosts enforce approved authorizations for logical access in accordance with the account privileges maintained locally for the account. Database accounts are managed local to the database schema, so that a user with access to one schema does not automatically have access to other schemas within the database. This is how users for one application are prohibited from accessing data associated with a separate system.

For application users, AFS HR Service Now uses its own Role Based Access Control (RBAC) model. The AFS HR Service Now administrators also have the ability to login to the application servers using their proper credentials to perform functions based on the permitted access.

Section 9: Privacy Act

9.1 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 and number *(list all that apply)*: Commerce Dept-18, Employee Personnel Files Not Covered by Notices of Other Agencies
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, a SORN is not being created.

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 periods of data contained in this system are covered by General Records Schedules #1. Civilian Personnel Records and have various retention periods for specific types of data. 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, whichever is 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		Overwriting	
Degaussing		Deleting	X
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

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.

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
X	**Moderate** – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	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: Name information is displayed as part of the process and securely archived within the information System.
	Quantity of PII	Provide explanation:
X	Data Field Sensitivity	Provide explanation: Fields within the form displayed Name information as part of the process. The information is securely archived within the information system.
	Context of Use	Provide explanation:
	Obligation to Protect Confidentiality	Provide explanation:
	Access to and Location of PII	Provide explanation:
	Other:	Provide explanation:

Section 12: Analysis

12.1 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.

12.2 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.

Appendix A – Privacy Act Notice Language

Authority to Collect

Includes the following, with all revisions and amendments: 5 U.S.C. 301; 44 U.S.C. 3101; 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.

Purpose

The web-based system contains support inquiries from users of Department of Commerce Human Resources Systems. Support staff will utilize the information to resolve inquiries regarding system functionality or status inquires. Information collected by this system may also be used for litigation, civil enforcement activities and criminal law enforcement activities.

Routine Uses

The Department will use this information in order to resolve customer inquiries. Disclosure of this information is permitted under the Privacy Act of 1974 (5 U.S.C. Section 552a) to be shared among Department staff for work-related purposes. Disclosure of this information is also subject to all of the published routine uses as identified in the Privacy Act System of Records Notice Commerce Dept-18, Employee Personnel Files Not Covered by Notices of Other Agencies.

Disclosure

Furnishing this information is voluntary; however, failure to provide accurate information may delay or prevent processing of inquiries.