Version Number: 01-2017

U.S. Department of Commerce
National Institute of Standards and Technology (NIST)

Privacy Impact Assessment for the Human Resource System (172-01)

Reviewed by: Susannah Schiller, 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

09/30/2019

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

U.S. Department of Commerce Privacy Impact Assessment
National Institute of Standards and Technology (NIST)

Unique Project Identifier: 172-01

<u>Introduction</u>: 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.

The Office of Human Resource Management (OHRM) is responsible for planning, developing, administering, and evaluating the human resources management programs of NIST and NTIS. This enables NIST to acquire and manage a dedicated, diverse, motivated, and highly qualified workforce to accomplish its mission and achieve its goals, while ensuring compliance with pertinent Federal, Office of Personnel Management, Office of Management and Budget, and Department of Labor, policy and administrative mandates.

(a) Whether it is a general support system, major application, or other type of system
The Human Resource System is a general support system.

(b) System location
The GRB component is a commercially hosted application located in Virginia. The HRSTAT component stores data in Florida and Virginia facilities within the continental United States. The remaining components are located at the NIST Gaithersburg, Maryland, and Boulder, Colorado, facilities within the continental United States.

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
The Performance System component shares information with the USDA National Finance Center (NFC) (for payroll processing).

(d) The way the system operates to achieve the purpose(s) identified in Section 4

1. Automated Reduction in Force (ARIF): Automates the reduction-in-force process for Human Resources staff from the selection of position(s) to be abolished, to the close of the case.
2. Performance System (Pay for Performance/General Workforce System): Provides the functionality for Human Resources staff, management, and administrative staff to record, document and report the annual employee performance rating, performance increase, bonus payout, and calculate the annual comparability increase. (ACI) for employees. Transmits updated data to the U.S. Department of Agriculture's (USDA) National Finance Center (NFC), which is the Department of Commerce's Payroll System of Record.
3. Human Resource Arrival/Departure System (HRADS): Processes Entrance on Duty

(EOD) and Departures, and automatically notifies other internal organizations of staffing changes.

4. Attachment Application: Serves as a temporary digital repository to collect forms and documents needed to process information regarding prospective and current federal employees. Once documents are finalized, the forms are manually uploaded into Office of Personnel Management's systems, and purged from the Attachment Application.
5. Government Retirement Benefits (GRB): Commercially hosted application that is used to perform employee retirement calculations based on salary and years of service. Upon an employee's request, authorized OHRM staff input the employee information into the system to perform the calculations.
6. HR STAT: Used to initiate and submit all Human Resources (HR) service requests to include completion and submission of HR forms, personnel action requests, and other HR requests.

(e) How information in the system is retrieved by the user

Information in the components is not directly accessible by the user. Prior to employment, individuals may update their information directly with Human Resources. After the initial Human Resources hiring process, employees have opportunity to review/update their information using the National Finance Center (NFC) Employee Personal Page (EPP).

(f) How information is transmitted to and from the system

The components of the system are only accessible on government issued computers through encrypted transmissions and are protected by multiple layers of firewalls. Each of the components permit assigning roles based on least privilege.

(g) Any information sharing conducted by the system

The Performance System component shares information with the USDA National Finance Center (NFC) (for payroll processing). The Attachment Application component shares information with the Office of Personnel Management.

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

National Institute of Standards and Technology Authorization Act of 2010 (Public Law 111-358, Title IV);

5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107;

5 U.S.C. 1302, 3109, 3301, 3302, 3304, 3305, 3306, 3307, 3309, 3313, 3317, 3318, 3319, 3326, 4103, 4723, 5532, and 5533, and Executive Order 9397.

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

__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.

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*	X	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	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: SSNs are required to process Human Resource transactions beginning with the recruitment of an employee and continuing until their separation from the federal government. The SSNs are also utilized for calculating the benefits within the GRB.					

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

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	X
b. Job Title	X	e. Email Address	X	h. Work History	X
c. Work Address	X	f. Business Associates	X		
i. 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	
b. IP Address	X	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	X	Hard Copy: Mail/Fax	X	Online	X
Telephone		Email			
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus	X	Other Federal Agencies	X
State, Local, Tribal		Foreign			
Other (specify):					

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.

Information in the components is not directly accessible by the user. Prior to employment, individuals may update their information directly with Human Resources. After the initial Human Resources hiring process, employees have opportunity to review/update their information using the National Finance Center (NFC) Employee Personal Page (EPP).

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
X	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	X
Other (specify):			

	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			
For a Computer Matching Program		For administering human resources programs	X
For administrative matters		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	
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).

1. The Automated Reduction in Force (ARIF) automates the reduction-in-force process from the selection of position(s) to be abolished, to the close of the case.
2. The Performance System (Pay for Performance/General Workforce System) administers recommended performance ratings/scores, increases, and bonuses, allowing generation of pay charts and comparability increase for employees.
3. The Human Resource Arrival/Departure System (HRADS) is used to process Entrance on Duty (EOD) and Departures and automatically notifies other internal organizations of staffing changes.
4. The Attachment Application workflow allows upload of attachments. The application is used as a temporary digital repository to collect forms and documents that are needed in support of prospective and current federal employees. Once documents are finalized, the forms are manually uploaded into Office of Personnel Management's systems, and purged from the Attachment Application.
5. Government Retirement Benefits (GRB) is a commercially hosted application that is used to perform employee retirement calculations based on salary and years of service. Upon an employee's request, authorized OHRM staff input the employee information into the system to perform the calculations.
6. HR STAT is used to initiate and submit all Human Resource (HR) service requests to include completion and submission of HR forms, personnel action requests, and other HR requests.

5.2 Describe any potential threats to privacy 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.)

Potential threats to privacy include the insider threat (e.g., authorized users misusing data or authorized user inadvertently combining multiple data sets resulting in aggregation of personal data).

Information collected is directly from the employee and is limited to only that which is needed for the service. Mitigating controls include employing and monitoring administrative access, training for administrators, and assurance of compliance to records management schedules.

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	X	X	
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 Performance System component pushes data to the USDA National Finance Center and is authorized to do so via an Interconnection Security Agreement.
	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			
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 a Privacy Act statement and/or privacy policy. The Privacy Act Statement and/or privacy policy can be found at: https://www.nist.gov/privacy-policy. A government warning banner is displayed when logging into the applications.	
	Yes, notice is provided by other means.	Specify how:
	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: For GRB component, individuals have the opportunity to decline to provide PII/BII. In doing so, their retirement benefits will not be calculated.
X	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: For the ARIF, Performance System, and HRADS components, employees may not decline after the initial Human Resources hiring process.

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.

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: Prior to employment, individuals may update their information directly with Human Resources. After the initial Human Resources hiring process, employees have opportunity to review/update their information using the National Finance Center (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: Access logs are kept and reviewed for anomalies.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): April 30, 2019 □ 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 supporting 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.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

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 components of the system are accessible on internal NIST networks protected by multiple layers of firewalls. Unauthorized use of the system is restricted by user authentication. Access logs are kept and reviewed for anomalies. For each component, PII is transferred in a secure fashion, and data-at-rest is encrypted. To guard against the interception of communication over the network, the components use the Transport Layer Security (TLS) protocol which encrypts communications between users' web browsers and the web server. Data that flows between the web server and the database server is secured through encrypted communication.

For the Performance System component, data shared with the National Finance Center uses FIPS 140-2 encrypted virtual private network technologies.

For the Attachment Application, data is scanned for viruses upon upload.

For the GRB application, user authentication and firewall administration is administered by the company.

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, number, and link. *(list all that apply)*: NIST-1 NIST Associates Commerce/DEPT-1 Attendance, Leave, and Payroll of Employees and Certain Other Persons Commerce/DEPT-18 Employee Personnel Files NOT Covered by Notices of Other Agencies OPM/GOVT-1 General Personnel Records OPM/GOVT-2 Employee Performance File Systems Records OPM/GOVT-3 Records of Adverse Actions, Performance Based Reductions in Grade and Removal Actions, and Terminations of Probationers OPM/GOVT-5 Recruiting, Examining, and Placement Records OPM/GOVT-7 Applicant Race, Sex, National Origin, and Disability Status Records
	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: General Records Schedule 1.0 General Records Schedule 2.0 Human Resources General Records Schedule 3.0 Technology
	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	X
Other (specify):			

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 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.
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: The data types that are collected and maintained can be used to identify specific individuals.
X	Quantity of PII	Provide explanation: The quantity of the PII that is collected and maintained pertains to all federal employees, past and present.
X	Data Field Sensitivity	Provide explanation: Personal identification numbers are used to identify individuals.
	Context of Use	Provide explanation:
X	Obligation to Protect Confidentiality	Provide explanation: The organization is legally obligated to protect the PII within the application.
X	Access to and Location of PII	Provide explanation: The information system is comprised of several applications that store and process PII.
	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.)

Potential threats to privacy include the insider threat (e.g., authorized users misusing data or authorized user inadvertently combining multiple data sets resulting in aggregation of personal data).

Information collected is directly from the employee and is limited to only that which is needed for the service. Mitigating controls include employing and monitoring administrative access, training for administrators, and assurance of compliance to records management schedules.

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

X	Yes, the conduct of this PIA results in required business process changes. Explanation: The Attachment Application enables HR staff to attach documents to customer service requests, which are then securely stored.
	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.