

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



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

Reviewed by: Del Brocket, 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: 2016.11.22 15:36:06 -05'00'

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)/Human Resource System

Unique Project Identifier: 172-01

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.

(a) A general description of the information in 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. The information in the system is defined in Section 2.

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

The following components within this system contain sensitive personally identifiable information:

1. Student Information System (SIS) - Allows an applicant to enter biographical information into the application to be considered for potential employment in the Student Volunteer Program (SVP) or the Summer High School Internship Program (SHIP). Management and administrative staff access the application to review potential candidates.
2. 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.
3. Performance System (Pay for Performance System/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) – the Department of Commerce's Payroll System of Record.
4. Human Resource Arrival/Departure System (HRADS) – Processes Entrance on Duty (EOD) and Departures, and automatically notifies other internal organizations of staffing changes.

- (c) Any information sharing conducted by the system

The Performance System component shares information with the USDA National Finance Center (for payroll processing).

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

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

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 defined in the following policy:

Department Organization Order 20-8, Director for Human Resources Management; Department Organization Order 30-2A, National Institute of Standards and Technology; Department Organization Order 30-7B, National Technical Information Service; and Department Administrative Order 202, Human Resources Management.

- (e) 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):					

- X This is an existing information system in which changes do not create new privacy risks.

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: SSN numbers are required to process Human Resource transactions beginning with the recruitment of an employee to their separation from the federal government.					

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): Bonus, pay increase information, series, grade, entry on duty (EOD) date, and separation date.					

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 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):			

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		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 Student Information System (SIS) allows an applicant to enter biographical information into the application to be considered for potential employment in the Student Volunteer Program (SVP) or the Summer High School Internship Program (SHIP).
2. 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.
3. The Pay for Performance System (PPS) administers recommended performance ratings/scores, increases, and bonuses, allowing generation of pay charts and comparability increase for employees.
4. 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.

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	
State, local, tribal gov't agencies			
Public			

Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

<input type="checkbox"/>	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. 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 general NIST 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. Specific to the Student Information System application, links to the Privacy Act Statement are also provided (see https://www-s.nist.gov/SIS/privacyStatement.cfm).	
	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 the SIS component, individuals have the opportunity to decline to provide PII/BII. In doing so, they will be ineligible for employment with NIST.
X	No, individuals do not have an	Specify why not: For the ARIF, Performance System, and

	opportunity to decline to provide PII/BII.	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's (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.
	Access to the PII/BII is being monitored, tracked, or recorded. Explanation:
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): January 29, 2016 <input type="checkbox"/> This is a new system.
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.
	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.

The system is 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 any anomalies. For each component, personally identifiable information 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 Secure Socket Layer (SSL) 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 technology.

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	<p>Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number (<i>list all that apply</i>):</p> <p>The National Bureau of Standards Authorization Act for Fiscal Year 1987m as amended, 15 U.S.C. 275 note Executive Order 9830, Amending the Civil Service Rules and Providing for Federal Personnel Administration</p> <p>SORN NIST/NIST-1 NIST Associates</p> <p>SORN Commerce/DEPT-1 Attendance, Leave, and Payroll of Employees and Certain Other Persons</p> <p>SORN Commerce/DEPT-18 Employees Personnel Files Not Covered by Notices of Other Agencies</p> <p>SORN OPM/GOVT-1 General Personnel Records</p> <p>SORN OPM/GOVT-2 Employee Performance File System Records</p> <p>SORN OPM/GOVT-3</p>
---	--

	Records of Adverse Actions, Performance Based Reductions in Grade and Removal Actions, and Terminations of Probationers SORN OPM/GOVT-5 Recruiting, Examining, and Placement Records SORN OPM/GOVT-7 Applicant Race, Sex, National Origin, and Disability Status Records
	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
	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 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. GRS 2.0 Human Resources (formerly GRS 1 and GRS 2) GRS 3.0 Technology (formerly GRS 20)
	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): There is an existing Department of Commerce Litigation hold on personnel records. In accordance with General Records Schedule 3.0, 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 General Records Schedule 2.0 authorize the disposition of records described herein.			

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: 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 applications.
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 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.