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

Privacy Threshold Analysis
for the
Human Resource System (172-01)
Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: Provide a general description of the information system in a way that a non-technical person can understand.

The E-Government Act of 2002 defines “information system” by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: “Information system” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

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 purpose that the system is designed to serve
   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.

e) The way the system operates to achieve the purpose
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.

f) A general description of the type of information collected, maintained, use, or disseminated by the system
The system contains identifying numbers, general personal data, and work-related data for NIST and NTIS government employees in order to process Human Resource transactions beginning with the recruitment of an employee and continuing until their separation from the federal government.

g) Identify individuals who have access to information on the system
NIST Human Resource federal employees have access to information within the components based on their role.

h) 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).

i) 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.

**Questionnaire:**

1. What is the status of this information system?

   ____ This is a new information system.  *Continue to answer questions and complete certification.*

   ____ This is an existing information system with changes that create new privacy risks.  

   *Complete chart below, continue to answer questions, and complete certification.*

   **Changes That Create New Privacy Risks (CTCNPR)**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Conversions</td>
<td>d. Significant Merging</td>
</tr>
<tr>
<td>b. Anonymous to Non-Anonymous</td>
<td>e. New Public Access</td>
</tr>
<tr>
<td>c. Significant System Management Changes</td>
<td>f. Commercial Sources</td>
</tr>
<tr>
<td>j. Other changes that create new privacy risks (specify):</td>
<td></td>
</tr>
</tbody>
</table>

   ____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.  *Continue to answer questions and complete certification.*

   ____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later).  *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

   NIST Special Publication 800-53 Revision 4, Appendix J, states “Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary.” Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

   ____ Yes.  *Please describe the activities which may raise privacy concerns.*

   ____ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?
As per DOC Privacy Policy: “For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as “trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential.” (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. “Commercial” is not confined to records that reveal basic commercial operations” but includes any records [or information] in which the submitter has a commercial interest and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.).”

Yes, the IT system collects, maintains, or disseminates BII about: (Check all that apply.)

Companies
Other business entities

No, this IT system does not collect any BII.

4. Personally Identifiable Information
4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: “The term ‘personally identifiable information’ refers to information which can be used to distinguish or trace an individual’s identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc...”

Yes, the IT system collects, maintains, or disseminates PII about: (Check all that apply.)

DOC employees
Contractors working on behalf of DOC
Members of the public

No, this IT system does not collect any PII.

If the answer is “yes” to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

Yes, the IT system collects, maintains, or disseminates PII other than user ID.

No, the user ID is the only PII collected, maintained, or disseminated by the IT system.
4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?
Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

____ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system’s Assessment and Authorization Package.
CERTIFICATION

__X__ I certify the criteria implied by one or more of the questions above apply to the Human Resource System (172-01) and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above do not apply to the Human Resource System (172-01) and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO): Teresa Whiteside

Signature of SO: ________________________________ Date: __________

Name of Information Technology Security Officer (ITSO): K. Robert Glenn

Signature of ITSO: ________________________________ Date: __________

Name of Co-Authorizing Official (AO): Susanne Porch

Signature of Co-AO: ________________________________ Date: __________

Name of Co-Authorizing Official (AO)/Bureau Chief Privacy Officer (BCPO): Susannah Schiller

Signature of Co-AO/BCPO: ________________________________ Date: __________