Privacy Threshold Analysis
for the
Applications Systems Division (ASD) Moderate Applications System
(183-01)
U.S. Department of Commerce Privacy Threshold Analysis
National Institute of Standards and Technology

Unique Project Identifier: 183-01

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 on 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 and its purpose 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).

The Applications Systems Division (ASD) Moderate Applications System provides the following enterprise-wide infrastructure components:

- The Central People Repository (CPR) is a collection of central database tables which contain information about NIST staff (i.e., Federal employee and Associate).
- The Web Content Management (WCM) component includes a public facing Organization of Scientific Area Committees (OSAC) Membership Application, which allows members of the public to apply for membership.
- The WebLogic component is an application infrastructure for developing, integrating, securing, and managing distributed applications.
- The Reporting Tools component provides reporting capabilities for various applications used throughout NIST.

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.

<table>
<thead>
<tr>
<th>Changes That Create New Privacy Risks (CTCNPRI)</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></td>
<td>g. New Interagency Uses</td>
</tr>
<tr>
<td></td>
<td>h. Internal Flow or Collection</td>
</tr>
<tr>
<td></td>
<td>i. Alteration in Character of Data</td>
</tr>
</tbody>
</table>

1
_X_ Yes.

Please describe the activities which may raise privacy concerns.

_X_ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

   Yes, the IT system collects, maintains, or disseminates BII about:
   
   ___ Companies
   ___ Other business entities

   _X_ 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)?

   Yes, the IT system collects, maintains, or disseminates PII about:
   
   _X_ DOC employees
   _X_ Contractors working on behalf of DOC
Members of the public

No, this IT system does not collect any PHI.

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

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

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

No, the user ID is the only PHI collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PHI is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PHI 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 PHI confidentiality impact level.

No, the context of use will not cause the assignment of a higher PHI 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 PIA 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 Application System Division (ASD) Moderate Applications System (183-01) 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 Application System Division (ASD) Moderate Applications System (183-01) and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Co-System Owner (SO):
Dale Little
Signature of SO: ___________________________ Date: 9/15/17

Name of Information Technology Security Officer (ITSO):
K. Robert Glenn
Signature of ITSO: ___________________________ Date: 9/14/17

Name of Co-Authorizing Official (AO):
Susannah Schiller, Acting
Signature of AO: ___________________________ Date: 9/14/17

Name of Co-Authorizing Official (AO)/Bureau Chief Privacy Officer (BCPO):
Susannah Schiller, Acting
Signature of AO/BCPO: ___________________________ Date: 9/14/17