Privacy Threshold Analysis
for the
Platform Services Division System (188-01)
U.S. Department of Commerce Privacy Threshold Analysis

National Institute of Standards and Technology (NIST)

Unique Project Identifier: 188-01

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. Sec: 44. U.S.C. § 3502(8).

a) Whether it is a general support system, major application, or other type of system

188-01 Platform Services is a general support system.

The Platform Services Division (PSD) System provides information technology platforms and services that directly support customer activities across NIST. The following components are included in the PSD System:

- Messaging Services (Email): Microsoft Messaging Services (Email) provides a tool for NIST information technology users to communicate.
- SharePoint: Microsoft SharePoint provides NIST information technology users a tool to help store, share, and manage digital information through: document management, workflow automation, web portals, etc.
- Customer Relationship Management (CRM): CRM enables NIST to manage interactions and relationships with customers, and review how NIST provides products, services, and support.
- Customer Relationship Management (CRM) eCommerce: CRM eCommerce enables a NIST storefront for the purchase and shipping of NIST products and services.

b) System location

- The Messaging Services (Email) component is located in the following Microsoft Government to Cloud datacenter locations: Santa Clara, California; Des Moines, Iowa; Boydton, Virginia; Chicago, Illinois; San Antonio, Texas; and Blue Ridge, Virginia facilities within the continental United States.
• The SharePoint and e-Approval components are located at the NIST Gaithersburg, Maryland facility within the continental United States.
• The CRM and CRM eCommerce components are located in San Francisco, California 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)
• To support account management across the services, NIST authorized user credentials are shared between these services and the NIST Identity, Credential, and Access Management (ICAM).
• To support transaction flow of eCommerce, the CRM connects with the Department of Treasury pay.gov service, and the Commerce Business System (CBS)/Core Financial System (CBS/CFS).

d) The purpose that the system is designed to serve
• The Messaging Services (Email) tool enables the sending and receiving of email communications between users and also permits digital signature and digital encryption options.
• The SharePoint component is a tool designed for collaboration. Authorized users can share information with one another for collaboration purposes related to job requirements.
• The eApproval component provides a framework where authorized users may populate, route (for signature), and archive data on authorized forms. Information is inputted by authorized users, routed for digital signature, and archived depending on rules defined by the end user.

e) The way the system operates to achieve the purpose
• Messaging Services (Email), SharePoint, and e-Approval solutions are used for administrative matters, to share information, to transact internal NIST business, and to promote information sharing initiatives.
• The CRM solution is used to improve federal services by allowing NIST to manage interactions and relationships with customers and review how NIST provides products, services, and support.
• The CRM eCommerce solution is used to improve federal services by offering an online storefront to sell NIST products and services to the public. Backend connectivity to the NIST Commerce Business System and the U.S. Department of Treasury pay.gov service handle the financial aspects of the transactions.

f) A general description of the type of information collected, maintained, use, or disseminated by the system
- Messaging Services (Email), SharePoint, and e-Approval permits storage of Work-Related Data, and may include personal photographs that user add to their profile.
- CRM collects General Personal Data and Work-Related Data.
- CRM eCommerce collects General Personal Data and Identifying Numbers (credit card and financial account).

g) Identify individuals who have access to information on the system
- Messaging Services (Email), SharePoint, and e-Approval are accessed by authorized NIST staff.
- The CRM component is accessed directly by authorized NIST users to retrieve information they are authorized to have.
- The CRM eCommerce component allows information to be retrieved by the person who registered and created an individual profile. Authorized NIST users retrieve information directly from the component.

h) How information in the system is retrieved by the user
- The Messaging Services (Email) tool enables the sending and receiving of email communications by and with users and permits digital signature when sent to other NIST users.
- Sharepoint sites can be accessed by authorized users to collaborate with each other.
- The eApproval component provides a framework where authorized users may initiate, route, and archive authorized forms (e.g., NIST internal form (DN or NIST), government standard forms (SF), DOC forms (CD), or other agency forms (OFI, OPM)). Information is inputted by authorized users, routed for digital signature, and archived depending on the rules defined by the initiator.
- The CRM component is accessed directly by authorized NIST users to retrieve data they are authorized to have.
- The CRM eCommerce component allows information to be retrieved by the person who registered and created an individual profile. Public users can only retrieve their own profile information. Authorized NIST users retrieve information directly from the component.

i) How information is transmitted to and from the system
- Messaging Services (Email), SharePoint, and e-Approval do not transmit information to or from other internal NIST systems. Information sharing is conducted within these systems between authorized users.
- The CRM component obtains information by (1) identifying people who have been invited to, registered for, and/or attended public conferences hosted by NIST; and (2) managing non-sensitive customer email and contact information copied by NIST staff from Microsoft Office 365, entered via a public facing form, or entered via a mobile application.
• The CRM eCommerce component provides an online NIST storefront where members of the public may purchase NIST products and services.

Questionnaire:

1. What is the status of this information system?

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

   X   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 (CTCNPR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Conversions</td>
</tr>
<tr>
<td>b. Anonymous to Non-Anonymous</td>
</tr>
<tr>
<td>c. Significant System Management Changes</td>
</tr>
<tr>
<td>j. Other changes that create new privacy risks (specify):</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.

   X   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.).”

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

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 Platform Services Division System (188-01) 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 Platform Services Division System (188-01) and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO):
Matt Wilkinson
Signature of SO: ____________________________ Date: 3-13-19

Name of Information Technology Security Officer (ITSO):
K. Robert Glenn
Signature of ITSO: ____________________________ Date: 3/13/19

Name of Co-Authorizing Official (AO):
Susannah Schiller
Signature of AO: ____________________________ Date: 3/13/19

Name of Co-Authorizing Official (AO)/Bureau Chief Privacy Officer (BCPO):
Susannah Schiller, Acting
Signature of AO/BCPO: ____________________________ Date: 3/13/19

7