Version Number: 01-2019

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

Privacy Threshold Analysis
for the
188-01 Platform Services System

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 (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

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
b) System location
c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
d) The purpose that the system is designed to serve
e) The way the system operates to achieve the purpose
f) A general description of the type of information collected, maintained, use, or disseminated by the system
g) Identify individuals who have access to information on the system
h) How information in the system is retrieved by the user
i) How information is transmitted to and from the system

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) is a general support system that 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.**

- **Teams: Microsoft Teams will replace Microsoft Skype as a tool that gives users the ability to communicate, share, and manage digital information. Moderate level PII is approved for sharing within the tool; however, any use of recordings in meetings or use of the chat feature is prohibited. All internal Microsoft Teams Owners are also required to sign a Rules of Behavior, and all Owners external to NIST will need approval from PSD.**
- **e-Approval: The e-Approval component replaces paper-based processes with: secure electronic forms, digital signatures, and workflow automation.**
- **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) and Teams components are 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 and Teams components are tools 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, Teams, and e-Approval solutions are used for administrative matters, to share information, to transact 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, Teams, and e-Approval permits use 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, Teams, and e-Approval are accessed by authorized NIST staff. Microsoft Teams also allows external users to gain access as Team Owners, but need authorization from PSD to do so.**
- **The CRM component is accessed directly by authorized NIST users to retrieve information 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 on it. 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 & Teams groups 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 on it. 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, Teams, and e-Approval do not transmit information to or from other internal NIST systems. Information sharing is conducted within these tools 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. The status of this information system:
   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 01-2017 or later). (Skip questions and complete certification.)

Changes That Create New Privacy Risks (CTCNPR)
Other changes that create new privacy risks:

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.

Activities
Other activities which may raise privacy concerns:

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.)."

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?
   As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

   The IT system collects, maintains, or disseminates PII about:

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

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.
Provide the legal authority which permits the collection of SSNs, including truncated form.

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

4d. 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.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d 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.

Is a PIA Required?	**Yes**

CERTIFICATION

X I certify the criteria implied by one or more of the questions above **apply** to the 188-01 Platform Services System 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 188-01 Platform Services System and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO):

Wilkinson, Matthew

Signature of SO: MATTHEW WILKINSON Digitally signed by MATTHEW WILKINSON Date: 2021.03.26 09:47:13 -04'00' Date: _____

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

Signature of Co-AO: ____N/A_____ Date: _____

Name of Information Technology Security Officer (ITSO):

Heiserman, Blair

Signature of ITSO: Digitally signed by BLAIR HEISERMAN Date: 2021.03.22 09:48:27 -04'00' Date: _____

Name of Authorizing Official (AO):

Sastry, Chandan

Signature of AO: CHANDAN SASTRY Digitally signed by CHANDAN SASTRY Date: 2021.03.26 14:17:03 -04'00' Date: _____

Name of Privacy Act Officer (PAO):

Fletcher, Catherine

Signature of PAO: CATHERINE FLETCHER Digitally signed by CATHERINE FLETCHER Date: 2021.04.20 10:41:20 -04'00' Date: _____

Name of Acting Bureau Chief Privacy Officer (BCPO):

Wilkinson, Matthew

Signature of Acting BCPO: MATTHEW WILKINSON Digitally signed by MATTHEW WILKINSON Date: 2021.03.26 09:46:46 -04'00' Date: _____