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

Privacy Impact Assessment
for the
188-01 Platform Services System

Reviewed by: Susannah Schiller, 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 PURVIS Digitally signed by CATRINA PURVIS
Date: 2020.11.19 17:40:15 -05'00' 11/19/2020

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)

Unique Project Identifier: 188-01

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) 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 way the system operates to achieve the purpose(s) identified in Section 4
(e) How information in the system is retrieved by the user
(f) How information is transmitted to and from the system
(g) Any information sharing conducted by the system
(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information
(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

a. Whether it is a general support system, major application, or other type of 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, and web portals. (Note: MS Teams includes OneDrive which is SharePoint on the backend platform.)**
- **Teams: Microsoft Teams will replace Microsoft Skype as a tool that gives users the ability to communicate, share, and manage digital information. PII is approved for sharing within the tool; however, any use of recordings in meetings 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) & 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 cloud-based 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 way the system operates to achieve the purpose(s) identified in Section 4

- **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.**
- **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.**

e. 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 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. Public users can only retrieve their own profile information. Authorized NIST users retrieve information directly from the component.**

f. 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.**

g. Any information sharing conducted by the system

- **Messaging Services (Email), SharePoint, Teams, and e-Approval manage user credentials by exchanging this information within the NIST 188-01 Active Directory Service.**
- **The CRM shares customer information with other internal NIST business units, specifically NIST 100-02, Associate Directors' Office System and NIST 480-01, MEP Enterprise Information System (MEIS) systems.**
- **The CRM eCommerce shares information with NIST 162-01, Commerce Business System, Core Financial System (CBS/CFS) and the U.S. Department of Treasury pay.gov service.**
- **NIST's use of Sharepoint provides the ability to collaborate/share documents with authorized users external to NIST.**

h. The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

The National Institute of Standards and Technology Act, as amended, 15 U.S.C. 271 et seq. (which includes Title 15 U.S.C. 272) and section 12 of the Stevenson-Wydler Technology Innovation Act of 1980, as amended, 15 U.S.C. 3710a.

5 U.S.C. 301; 35 U.S.C. 2; the Electronic Signatures in Global and National Commerce Act, Public Law I 06-229; 28 U.S.C. 533-535; 44 U.S.C. 1301; Homeland Security Presidential Directive 12 and IRS Publication-1075.

i. The Federal Information Processing Standards (FIPS) 199 security impact category for the system is **Moderate.**

Section 1: Status of the Information System

1.1 The status of this information system:

This is an existing information system in which changes create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2017 or later).

Changes That Create New Privacy Risks (CTCNPR)
Microsoft Teams will replace Microsoft Skype as a tool that gives users the ability to communicate, share, and manage digital information. NIST's use of Sharepoint provides the ability to collaborate/share documents with authorized users external to NIST.
Other changes that 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.

Identifying Numbers (IN)
Other identifying numbers:
Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:

General Personal Data (GPD)
Name
Home Address
Telephone Number
Email Address
Other general personal data:

Work-Related Data (WRD)
Occupation
Job Title
Work Address
Work Telephone Number
Work Email Address
Work History
Business Associates
Other work-related data:

Distinguishing Features/Biometrics (DFB)
Photographs
Other distinguishing features/biometrics:

System Administration/Audit Data (SAAD)
User ID

IP Address
Date/Time of Access
Queries Run
Other system administration/audit data:

Other Information
Although other PII is not solicited, collected, maintained, or disseminated, it is possible for individuals to voluntarily make such information available.

2.2 Indicate sources of the PII/BII in the system.

Directly from Individual about Whom the Information Pertains
In Person
Telephone
Hard Copy - Mail/Fax
Email
Online
Other:

Government Sources
Within the Bureau
Other:

Non-government Sources
Other:

2.3 Describe how the accuracy of the information in the system is ensured.

Messaging Services (Email), SharePoint, Teams, and e-Approval: Information system integrity controls and NIST user management of their information.

CRM: Information system integrity controls. Users can contact NIST (e.g., https://www.nist.gov/about-nist/contact-us) to review/update their PII.

CRM eCommerce: Information system integrity controls. Users can review/update their individual profile through the online NIST storefront portal.

2.4 Is the information covered by the Paperwork Reduction Act?

No, the information is not covered by the Paperwork Reduction Act.
The OMB control number and the agency number for the collection:

2.5 Is there any technology used that contain PII/BII in ways that have not been previously deployed?

No

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)
Other:

Section 3: System Supported Activities

3.1 Are there any IT system supported activities which raise privacy risks/concerns?

No, there are not any IT system supported activities which raise privacy risks/concerns.

The IT system supported activities which raise privacy risks/concerns.

Activities
Other:

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated.

Purpose
For administrative matters
To improve Federal services online
To promote information sharing initiatives
For employee or customer satisfaction
Other:

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).

Messaging Services (Email) is for use by NIST employees and associates to exchange information between themselves and with the public.

SharePoint & Teams are tools supporting collaboration and information sharing between authorized users.

eApproval is used by NIST employees to route and digitally sign electronic forms.

CRM is for use by authorized NIST staff to centralize and aggregate data regarding its customer base and their interest areas, permitting insight into interactions and relationships with a customer and/or business, thus allowing NIST to better understand customer needs. The non-sensitive PII in the CRM may be about federal employees, federal contractors, foreign nationals, members of the public, or partners and stakeholders.

CRM eCommerce provides a NIST storefront where members of the public may purchase NIST products and services. The PII collected is used to pay for and deliver these products and services.

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

Unauthorized access could result in a breach of users' information. Information system security controls used to protect this information are implemented, validated, and continuously monitored. NIST user access is restricted to authorized users. Annual training and rules of behavior are provided to internal users on the appropriate handling of PII. The components have records schedules and procedures in place to dispose of data accordingly. **Unauthorized use of CRM could result in a breach of user's information. This risk is minimized through annual training to users and annual signing of rules of behavior, which includes consequences of actions. In addition, risk is minimized through limiting the number of authorized users.**

Section 6: Information Sharing and Access

6.1 Will the PII/BII in the system be shared?

Yes, the PII/BII in the system will be shared

The recipients the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared.

Direct Access - Federal agencies **Direct Access - Within the bureau** **Direct Access – Public (authorized users only)**
Other:
Law Enforcement.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII.
The name of the IT system and description of the technical controls which prevent PII/BII leakage:
Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. **Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:** **CRM:** • **NIST 100-02, Associate Directors' Office System** • **NIST 480-01, MEP Enterprise Information System (MEIS)** **CRM eCommerce:** • **NIST 162-01, Commerce Business System, Core Financial System (CBS/CFS)**

- **U.S. Department of Treasury pay.gov**

Technical controls are identified in Section 8.2.

6.3 Identify the class of users who will have access to the IT system and the PII/BII.

Class of Users
General Public
Government Employees
Contractors
Other:

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.

Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.

Yes, notice is provided by a Privacy Act statement and/or privacy policy.

Yes, notice is provided by other means.

No, notice is not provided.

The Privacy Act statement and/or privacy policy can be found at:

The general NIST Privacy Policy can be found at https://www.nist.gov/privacy-policy. A Privacy Act Statement is also provided on the CRM eCommerce profile registration page.

The reason why notice is/is not provided:

CRM: Notice is provided on the web form interface where inquiries are received by the public. Notice is also provided verbally when obtaining information in person.

Messaging Services (Email), SharePoint, and e-Approval: Not applicable.

Teams: Notice is provided to all members via Warning Banner. Rules of Behavior is also signed by all Team Owners.

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

Yes, individuals have an opportunity to decline to provide PII/BII.
No, individuals do not have an opportunity to decline to provide PII/BII.

The reason why individuals can/cannot decline to provide PII/BII:

Yes:

CRM: Individuals have the opportunity to decline to provide PII by not submitting a public inquiry or by not providing contact information. In doing so, they will not be able to obtain responses to inquiries with

NIST and may not be able to transact business with NIST.

CRM eCommerce: A customer may decline to provide his/her PII, but then he/she will not be able to purchase NIST products and services. Products and services are targeted to scientific users, rather than the general public, and written acceptance of terms of use are required by NIST for the offered products and services.

Messaging Services (Email), SharePoint, Teams, and e-Approval: All users can choose not to share any PII/BII.

Federal requirements subject users to monitoring. Users are required to agree to monitoring in general account rules of behavior before account credentials are issued.

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.
The reason why individuals can/cannot consent to particular uses of their PII/BII:
Yes: **CRM: Opportunity to consent to particular uses of PII is provided on the web form interface where inquiries are received by the public. Notice is also provided verbally when obtaining information in person.** **CRM eCommerce: Customers have the ability to consent to particular uses of their individual profile information upon registration.** **Messaging Services (Email), SharePoint, Teams, and e-Approval: Users do have the opportunity to consent to particular uses of their PII/BII.** **Federal requirements subject users to monitoring. Users are required to agree to monitoring in general account rules of behavior before account credentials are issued.**

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

Yes, individuals have an opportunity to review/update PII/BII pertaining to them.
The reason why individuals can/cannot review/update PII/BII:
Yes: **CRM: Opportunity to review/update PII is available through the person and/or system to whom they originally gave their information, or through the NIST external web portal at https://www.nist.gov/about-nist/contact-us.** **CRM eCommerce: Customers have the ability to review/update their individual profile information through the NIST storefront.** **Messaging Services (Email), SharePoint, Teams, and e-Approval: Any PII submitted can be reviewed/updated.** **Individual's data for information technology security incidents are not modified in case there is a need to provide for human resource or legal examination.**

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system.

All users signed a confidentiality agreement or non-disclosure agreement.

All users are subject to a Code of Conduct that includes the requirement for confidentiality.

Staff (employees and contractors) received training on privacy and confidentiality policies and practices.

Access to the PII/BII is restricted to authorized personnel only.

Access to the PII/BII is being monitored, tracked, or recorded.

The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements.

The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.

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 (POA&M).

A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.

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.

Reason why access to the PII/BII is being monitored, tracked, or recorded:

Access logs are kept and reviewed for anomalies.

The information is secured in accordance with FISMA requirements.

Is this a new system? No
Below is the date of the most recent Assessment and Authorization (A&A).
04/30/2020

Other administrative and technological controls for the system:

8.2 General description of the technologies used to protect PII/BII on the IT system. *(Includes data encryption in transit and/or at rest, if applicable).*

Messaging Services (Email), SharePoint, Teams, and e-Approval:

The components of the system are accessible on internal NIST networks protected by multiple layers of firewalls. Remote access is provided through FIPS 140-2 encrypted virtual private network technologies. Unauthorized use of the system is restricted by user authentication, account management processes, and segregation of privileged user accounts and devices. Access logs are kept and reviewed for anomalies.

To guard against the interception of communication over the network, the components use the Transport Layer Security (TLS) protocol which encrypts communications between users' web browsers and the web

server (i.e., Messaging Services (Email) web client, SharePoint, Teams, and eApproval).

Digital signature and data encryption of the data is available in Messaging Services (Email) and eApproval components through the use of PIV credentials. Data is encrypted at rest (i.e., completed eApproval forms).

For the Messaging Services (Email), Data Loss Prevention (DLP) is employed on attachments, message subject and body. Advance Threat Protection is also employed on email accounts.

CRM and CRM eCommerce:

The CRM and CRM eCommerce components are hosted by a cloud vendor that has a FedRAMP issued Authority to Operate. Data is stored at the vendor's storage sites, which are within the continental United States. Data-at-rest encryption is employed using CRM's FIPS validated encryption (AES 128) on selected data fields. Access logs are kept and reviewed for anomalies.

There is a public facing web interface which permits anyone to submit information into CRM. The interface uses the Secure Socket Layer (SSL) protocol, and thus encrypts data flowing between the web interface and the backend CRM. Interface fields restrict data input. All other access to CRM requires NIST-issued credentials because access is restricted by user authentication.

Remote NIST users access CRM by first connecting to the NIST network through a Virtual Private Network (VPN). Mobile device users may utilize a CRM mobile application which allows a direct front-end into the CRM, using the TLS 1.2 protocol, encrypting end-to-end communication.

To mitigate risk associated with mobile devices, only Government-furnished equipment (NIST-owned) may be used with the mobile application. Attachments can be viewed, not downloaded locally to the device. NIST mobile devices require full device encryption and mobile device management (MDM). MDM uses full device FIPS validated encryption on Android devices, and FIPS validated encryption or encryption that is in process for FIPS validation for iOS devices. MDM also enforces inactivity periods, password management, etc.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

Yes, the PII/BII is searchable by a personal identifier.

9.2 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."

Yes, this system is covered by an existing system of records notice (SORN).
SORN name, number, and link:
Commerce/DEPT-2 **Accounts Receivable** **Commerce/DEPT-23** **Information Collected Electronically in Connection with Department of Commerce Activities, Events, and Programs** **Commerce/DEPT-25** **Access Control and Identity Management System**

SORN submission date to the Department:

Section 10: Retention of Information

10.1 Are these records are covered by an approved records control schedule and monitored for compliance?

Yes, there is an approved record control schedule.
Name of the record control schedule:
GRS 3.0 Technology **GRS 4.2 Information Access and Protection Records** **GRS 5.2/020 Intermediary Records** **GRS 5.8 Administrative Help Desk** **GRS 6.5 Public Customer Service Records**
The stage in which the project is in developing and submitting a records control schedule:
Yes, retention is monitored for compliance to the schedule.
Reason why retention is not monitored for compliance to the schedule:

10.2 Indicate the disposal method of the PII/BII.

Disposal
Shredding **Overwriting** **Degaussing** **Deleting**
Other disposal method of the PII/BII:

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

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. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

11.2 The factors that were used to determine the above PII confidentiality impact levels.

Factors that were used to determine the above PII confidentiality impact levels	Explanation
Identifiability **Quantity of PII** **Data Field Sensitivity** **Context of Use** **Access to and Location of PII** **Other**	**Identifiability** **The data types in the CRM solution that are collected and maintained can be used to identify specific individuals and businesses, and their NIST interests.** **Quantity of PII** **The volume of data transmitted that may include other personally identifiable information is unknown. The quantity of the**

	PII in the CRM solution that is collected pertains to federal employees, federal contractors, foreign nationals, members of the public, or partners and stakeholders. **Data Field Sensitivity** **eApproval: Once populated by the end user, forms within the eApproval component may contain PII/BII. Each field within data inputs is reviewed for sensitivity. Access to data is restricted to just those NIST users that need to review and/or sign a specific form.** **CRM: requires General Personal Data.** **CRM eCommerce: uses the U.S. Department of Treasury pay.gov to collect payment information.** **Context of Use** **Messaging Services & Teams: Use of photographs within Messaging Services (Email) or Teams is at the end user's judgement/discretion.** **CRM: enables NIST to manage interactions and relationships with their customers, and review how NIST provides products, services, and support.** **CRM eCommerce: allows a centrally managed eCommerce solution.** **Access to and Location of PII** **The CRM and CRM eCommerce function uses a cloud-based solution.** **Other** **The aggregation of the various data inputs is considered.**

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

The threat of unauthorized access and/or misuse exists but is reduced by effective security controls, internal user training and requiring internal users to sign relevant rules of behavior agreements.

A risk exists with authorized users inputting inaccurate information into the CRM component. This risk is mitigated through internal user training. A risk also exists with the general public inputting incorrect information into the CRM eCommerce solution. This risk is mitigated by allowing the general public to redress their information. In addition, the input field parameters have been limited in size to mitigate excessive input by the customer. **The CRM eCommerce functionality replaces several different existing on-premise systems, but includes no new use of information from already approved solutions. This reduces the need to implement additional eCommerce solutions for new requirements.** **The use of U.S. Department of Treasury pay.gov service eliminates NIST need to store and process users' information locally, reducing risk associated with users' financial information.**

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

No, the conduct of this PIA does not result in any required business process changes.
Explanation

12.3 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
Microsoft Teams will replace Microsoft Skype.