Version Number: 01-2019

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

Privacy Impact Assessment
for the
640-01 Office of Reference Materials (ORM) System

Reviewed by: Claire Barrett, 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

Jennifer Goode 09/29/2021

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: 640-01

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 system is a general support system.

b. System location
The system is located at the NIST Gaithersburg, Maryland facility 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 SRM Business System ("Limestone") connects to the internal NIST 162-01 Commerce Business System (CBS)/Core Financial System (CBS/CFS) for invoicing and accounting, and the internal shipping system.

Limestone also has an interconnection with the NIST Salesforce e-commerce system. Limestone initiates all connections with Salesforce using custom developed APIs; Salesforce does not reach into NIST 640-01 Limestone internally at all.

d. The way the system operates to achieve the purpose(s) identified in Section 4
The Office of Reference Materials (ORM) System improves federal services online through two components:

- **The SRM Business System ("Limestone") is the internal application used to manage inventory of SRMs and process orders for the public's acquisition of NIST products and services (i.e., NIST Standard Reference Data (SRD), Standard Reference Materials (SRM), Standard Reference Instruments (SRI)).**
- **The Online Request System (ORS) is a web-based application that allows external users to purchase SRMs online in an efficient, secure, and user-friendly manner. The SRM ORS consists of an internal administrative component, as well as an external public-facing component. All payments for products purchased through the SRM ORS are processed internally by the NIST Accounting Department.**

e. How information in the system is retrieved by the user
The system allows information to be retrieved by the customer who registered and created an individual or organizational profile (e.g., account). 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
The system encrypts all information in transmission and at rest. The SRM ORS transmits customer order requests to Limestone. All processing and data storage within Limestone is encrypted and resides within NIST Gaithersburg.

g. Any information sharing conducted by the system
The Limestone application connects with the internal NIST 162-01 Commerce Business System (CBS)/Core Financial System (CBS/CFS) for invoicing and accounting, and the internal shipping system.

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 275) and section 12 of the Stevenson-Wydler Technology Innovation Act of 1980, as amended, 15 U.S.C. 3710a.;

Public Law 90-396, July 11, 1968, The Standard Reference Data Act;

5 U.S.C. 5701-5709 and 5721-5739, 28 U.S.C. 3101-3105, Debt Collection Act of 1982 (Pub. L. 97-365); 26 U.S.C. 6402(d); and 31 U.S.C. 3711.

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 do not 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)

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)
Taxpayer ID
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)
Work Address
Work Telephone Number
Work Email Address
Other work-related data:

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

System Administration/Audit Data (SAAD)
IP Address
Date/Time of Access
Other system administration/audit data:

Other Information

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

Directly from Individual about Whom the Information Pertains
Telephone
Email
Online

Other:

Government Sources
Within the Bureau
Other:

Non-government Sources
Public Organizations **Private Sector**
Other:

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

The ORS portal accepts customer data directly from users (i.e., public customers) for the purchase of NIST goods/materials, and they can review/update their profile through the ORS portal. Data is also reviewed by NIST staff to ensure fulfillment of the order. **All necessary security controls are in place to ensure encryption standards are met including data encrypted at rest and in transit.**

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

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**
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).

Customers of the ORS are public or private individuals, companies, or academic institutions.

The public customer selects products or services for purchase and sets up an individual or organizational profile (e.g. account). Subsequent payment information to enable supporting financial activities (e.g., invoicing, tracking, payment) is not stored on this system, but utilizes pay.gov. Information regarding the purchase is tracked for programmatic and mission activities (e.g., supply/demand, communities who purchase, etc.).

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.)

Potential threats to privacy include the insider threat (e.g., authorized users misusing data or authorized user inadvertently combining multiple data sets resulting in aggregation of personal data).

Information collected is directly from the customer and is limited to only that which is needed for the service. Mitigating controls include employing and monitoring administrative access, training for administrators, and assurance of compliance to records management schedules. Information system security controls used to protect this information are implemented, validated, and continuously monitored.

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.

Bulk Transfer - Within the bureau **Case-by-Case - Within the bureau** **Direct Access - Within the bureau**
Other:

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:
NIST 162-01 Commerce Business System, Core Financial System (CBS/CFS) **NIST 188-01 Platform Services Division (PSD) System** **NIST 138-01 Business Operations Office (BOO) System**

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

Class of Users
Government Employees
Other:
Public customers have access to their own PII.

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.**
The Privacy Act statement and/or privacy policy can be found at:
The Privacy Act statement and/or privacy policy can be found at: _https://www.nist.gov/policies-notices. **A Privacy Act Statement is found on customer registration profile pages: https://shop.nist.gov, https://www-s.nist.gov/srmors/login.cfm?checkout=, https://www-s.nist.gov/srmors/new_user.cfm, or https://www-s.nist.gov/srd_online/index.cfm?fuseaction=home.restrictedPage (Note: the Privacy Act Statement is presented in the shopping cart after selection of a product)**
The reason why notice is/is not provided:

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.
The reason why individuals can/cannot decline to provide PII/BII:
Individuals choose whether to place an order or request a service. In order to initiate the order or service, PII/BII must be provided. The individual can choose to decline to provide PII/BII and not complete an order or request a service.

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

No, individuals do not 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:
If an individual chooses to provide their PII/BII for an order or to request a service, there is no additional consent requested of that individual for particular uses of their PII/BII.

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:
Customers also have opportunity to review/update their information within the individual or enterprise account profile they established in the ORS at anytime during the ordering process.

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system.

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.**
Reason why access to the PII/BII is being monitored, tracked, or recorded:
Access logs are kept and reviewed for anomalies on an as needed basis.
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).** **7/31/2021**
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).*

The ORS uses standard approved encryption protocols, and all proper security controls are in place. **The applications are administratively accessible on internal NIST networks protected by multiple layers of firewalls. Unauthorized use of the system is restricted by user authentication. Access logs are kept and reviewed for anomalies on an as needed basis. Data is stored on servers located at the NIST Gaithersburg,**

Maryland facility within the continental United States. **To guard against the interception of communication over the network, the components use the Transport Layer Security (TLS) protocol which encrypts communications, or FIPS 140-2 encrypted virtual private network technologies between organizations and the public. System administration requires privileged access, which employs additional protective measures. Access to the administrative interface is limited to hardware using a NIST IP address, combined with user authentication (NIST-issued credentials).**

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:
DEPT-2, Accounts Receivable **DEPT-23, Information Collected Electronically in Connection with Department of Commerce Activities, Events, and Programs**
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 5.2/020 Intermediary Records **GRS 6.5/020 Customer\client records** **NIST Comprehensive Records Schedule Item 31 (maintains standard reference material 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
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.)*

Low – 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
Quantity of PII **Data Field Sensitivity** **Context of Use**	**Quantity of PII-A Taxpayer Identification Number (TIN) is an identification number used by the Internal Revenue Service (IRS) in the administration of tax laws. It is issued either by the Social Security Administration (SSA) or by the IRS. A Social Security number (SSN) is issued by the SSA whereas all other TINs are issued by the IRS.** **Data Field Sensitivity-Customer's Financial Account information.** **Context of Use-Customer's providing information to obtain a product or service.**

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.)

Threats could arise from having multiple storefronts and subsequently multiple systems to transact eCommerce. NIST centralized its eCommerce systems into a single system to ensure consistency with management, administration, and technical controls.

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.

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