

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



**Privacy Threshold Analysis  
for the  
640-01 Office of Reference Materials (ORM) System**

## U.S. Department of Commerce Privacy Threshold Analysis National Institute of Standards and Technology (NIST)

**Unique Project Identifier: 640-01**

**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*

**The system is a general support system.**

b. *System location*

**The system is located in San Francisco, California within the continental United States, and 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 system is a standalone system.*

**The NIST Storefront application connects with the Department of Treasury pay.gov service to process credit card orders, and the internal NIST 162-01 Commerce Business**

**System (CBS)/Core Financial System (CBS/CFS) for invoicing and accounting, and the internal shipping system.**

*d. The purpose that the system is designed to serve*

**The purpose is to improve federal services online, while providing the requisite capabilities for administration of the service.**

*e. The way the system operates to achieve the purpose*

**The Office of Reference Materials (ORM) System improves federal services online through two components:**

- **The NIST Storefront is an e-Commerce application 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), and Calibration Support System (CSS)). The e-Commerce application includes inventory, order, and purchase through the NIST Storefront (<https://shop.nist.gov>).**
- **The CSS is internal facing, and permits documentation of equipment, calibration procedures, and business and payment information for businesses requesting calibration services.**

*f. A general description of the type of information collected, maintained, use, or disseminated by the system*

**Identifying numbers (IN), general personal data (GPD) and work-related data (WRD) to support the purchase of products and services from NIST. Public purchase may be from an individual or organization.**

*g. Identify individuals who have access to information on the system*

**Public customers have access to register and create an individual or organizational profile (e.g., account). Authorized NIST users access information based on their role.**

*h. 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 based on their role.**

*i. How information is transmitted to and from the system*

**After a public customer places an order within the system, administrators fulfill the order and prepare for shipping. SRD e-Commerce customers receive an email after an order is complete, with a link to download the data products. SRD e-Commerce customer service agents use an internal portal to manage customer orders and to provide customer service.**

**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?	<b>Yes</b>
--------------------	------------

## CERTIFICATION

X I certify the criteria implied by one or more of the questions above **apply** to the 640-01 Office of Reference Materials (ORM) 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 640-01 Office of Reference Materials (ORM) System and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO):

Choquette, Steven

Signature of SO: \_\_\_\_\_ Date: \_\_\_\_\_

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

Lin, Eric

Signature of Co-AO: \_\_\_\_\_ Date: \_\_\_\_\_

Name of Information Technology Security Officer (ITSO):

Glenn, K. Robert

Signature of ITSO: \_\_\_\_\_ Date: \_\_\_\_\_

Name of Authorizing Official (AO):

Sastry, Chandan

Signature of AO: \_\_\_\_\_ Date: \_\_\_\_\_

Name of Privacy Act Officer (PAO):

Fletcher, Catherine

Signature of PAO: \_\_\_\_\_ Date: \_\_\_\_\_

Name of Bureau Chief Privacy Officer (BCPO):

Schiller, Susannah

Signature of BCPO: \_\_\_\_\_ Date: \_\_\_\_\_