

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



**Privacy Threshold Analysis  
for the  
141-01 Commerce Standard Acquisition and Reporting System  
(CSTARS)**

## U.S. Department of Commerce Privacy Threshold Analysis

### National Institute of Standards and Technology (NIST)

**Unique Project Identifier: 141-01**

**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 brief description of the information system.*

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*

**The Commerce Standard Acquisition Reporting System (CSTARS) enables a standard business practice in accordance with the U.S. Department of Commerce (DOC). It is comprised of the following component:**

- **CSTARS: The workflow to create, route, track, and report all procurement activity at NIST is supported using two modules: C.Request and C.Award. The system includes small purchase requirements, as well as complex contract activities.**

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

**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 CSTARS connects with or receives information from the following information systems:**

- **General Services Administration Federal Procurement Data System - Next Generation;**
- **General Services Administration System for Award Management (SAM);**
- **General Services Administration System Federal Business Opportunities (FedBizOpps);**
- **Office of Management and Budget MAX, Department of Commerce Acquisition Data Warehouse;**
- **NOAA1101, Information Technology Center (ITC) General Support System (GSS) Commerce Business System component;**
- **NIST 162-01, Commerce Business System, Core Financial System (CBS/CFS); and**
- **NIST 188-01, Platform Services System (ServiceNow)**

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

**CSTARS enables a standard business practice for all procurement activity conducted by NIST. The system includes small purchase requirements, as well as complex contract activities.**

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

**CSTARS is supported through two modules, C.Request and C.Award, and enables a workflow to create, route, track, and report all procurement activity conducted by NIST and DOC bureaus serviced by NIST.**

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

**The following are examples of transactions using CSTARS which may contain Personally Identifiable Information (PII) or Business Identifiable Information (BII):**

- **Creation of a purchase request by a supported Commerce agency;**
- **Route purchase request for approval and award;**
- **Track, report, and close-out of acquisition activity; and**
- **Responses to RFI (Request for Information), RFQ (Request for Quote), or RFP (Request for Proposal).**

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

**NIST and DOC employees/contractors.**

***h.) How information in the system is retrieved by the user***

**CSTARS information is retrieved within the applications by document/order numbers, by contracting officer/requester/user, and group as defined with the application.**

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

**To guard against the interception of communication over the network, the component uses the Transport Layer Security (TLS) protocol, which encrypts communications between users' web browsers and the hosting server. In addition, data is sent from the system using Secure File Transfer Protocol (SFTP)/Secure Shell (SSH) protocols.**

**Questionnaire:**

## 1. Status of the Information System

## 1a. What is 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:

## 1b Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

## 2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Rev. 5, 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 sensitive 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 sensitive 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 SAOP approved PIA must be a part of the IT system’s Assessment and Authorization Package.***

Is a PIA Required?	Yes
--------------------	-----

## CERTIFICATION

**X** The criteria implied by one or more of the questions above **apply** to the 141-01 Commerce Standard Acquisition and Reporting System (CSTARS) and as a consequence of this applicability, a PIA will be performed and documented for this IT system.

The criteria implied by the questions above **do not apply** to the 141-01 Commerce Standard Acquisition and Reporting System (CSTARS) and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

<b>Information System Security Officer or System Owner</b>  Name: Widdup, Joseph Office: 301/B130 Phone: 301-975-2580 Email: joseph.widdup@nist.gov   Signature: _____  Date signed: _____	<b>Chief Information Security Officer</b>  Name: Heiserman, Blair Office: 225/A155 Phone: 301-975-3667 Email: nist-itso@nist.gov   Signature: _____  Date signed: _____
<b>Co-Authorizing Official</b>  Name: Folk, Alex Office: 225/B259 Phone: 301-975-8089 Email: alex.folk@nist.gov   Signature: _____  Date signed: _____	<b>Authorizing Official</b>  Name: Sastry, Chandan Office: 225/B222 Phone: 301-975-6500 Email: chandan.sastry@nist.gov   Signature: _____  Date signed: _____
<b>Privacy Act Officer</b>  Name: Fletcher, Catherine Office: 101/A523 Phone: 301-975-4054 Email: catherine.fletcher@nist.gov   Signature: _____  Date signed: _____	<b>Chief Privacy Officer</b>  Name: Barrett, Claire Office: 225/B226 Phone: 301-975-2852 Email: claire.barrett@nist.gov   Signature: _____  Date signed: _____