Version Number: 01-2019

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

## Privacy Impact Assessment
## for the
## 141-01 Commerce Standard Acquisition and Reporting System (CSTARS)

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

Jennifer Goode for Dr. Catrina D. Purvis 10/04/2020

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: 141-01**

**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*

**The Commerce Standard Acquisition Reporting System (CSTARS) enables a standard business practice in which the workflow to create, route, track, and report all procurement activity 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)**
- **NIST 188-01 Platform Services System (ServiceNow)**

*d. The way the system operates to achieve the purpose(s) identified in Section 4*
**The Commerce Standard Acquisition Reporting System (CSTARS) enables a standard business practice in which the workflow to create, route, track, and report all procurement activity at NIST and DOC bureaus serviced by NIST is accomplished.**

*e. 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.**

*f. How information is transmitted to and from the system*
**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 hosting server. In addition, data is sent from the system using SFTP/SSH protocols.**

*g. Any information sharing conducted by the system*
**Data is shared with other DOC agencies who utilize NIST acquisition support, as well as the DOC Office of Inspector General for purposes of fraud analysis. Data is also shared as follows:**

- **DOC agencies for which NIST provides acquisition services include: NIST, National Technical Information System (NTIS), Bureau of Industry and Security (BIS), Economic Development Administration (EDA), International Trade Agency (ITA), Office of Inspector General (OIG), Minority Business Development Agency (MDBA), and National Telecommunications & Information Administration (NTIA). However, at this point most DOC bureaus have transitioned to being serviced by the DOC Office of Secretary, Enterprise Service group**
- **General Service Administration Federal Procurement Data System - Next Generation (FPDS-NG)**
- **General Service Administration System of Award Management (SAM) for vendor information;**
- **General Service Administration Federal Business Opportunities (FedBizOpps) for procurement information;**
- **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; and**
- **Other internal NIST business units (NIST 162-01 & NIST 188-01).**

**Data is shared with other Government entities on a case-by-case basis for purposes of fraud, audit, or law enforcement.**

*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.; The "Federal Information Security Management Act of 2002 (FISMA).**

**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**<br>**Credit Card** |
| Other identifying numbers: |
| |
| Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form: |
| **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 used by the SSA whereas TINS are issued by the IRS.**<br><br>**Government Purchase Cards, not personal credit cards.** |

| |
|---|
| |

| General Personal Data (GPD) |
|---|
| **Name** |
| **Home Address** |
| **Telephone Number** |
| **Email Address** |
| **Other general personal data** |
| Other general personal data: |
| **Information is used if a sole proprietor registers using this information in the General Services Administration's System for Award Management (SAM).** |

| Work-Related Data (WRD) |
|---|
| **Occupation** |
| **Work Address** |
| **Work Telephone Number** |
| **Work Email Address** |
| **Salary** |
| **Other work-related data** |
| Other work-related data: |
| **Other work related data: DUNS identifier** |

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

| System Administration/Audit Data (SAAD) |
|---|
| **User ID** |
| **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 |
|---|
| |
| Other: |
| |

| Government Sources |
|---|
| **Within the Bureau** |
| **Other DOC Bureaus** |
| **Other Federal Agencies** |
| Other: |
| |

| Non-government Sources |
| --- |
| **Private Sector** |
| **Other** |
| Other: |
| **Responses to RFI (Request for Information), RFQ (Request for Quote), or RFP (Request for Proposal)** |

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

| |
| --- |
| **Originating data inaccuracies are corrected via access and redress controls. In turn, this corrected data is pulled into the CSTARs 141-01 system as accurate data. CSTARs has several checks through the agreement process including involvement from the data source (public) to verify accuracy. This ensures the highest data integrity/quality on CSTARs partners is maintained.** |

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** |
| 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).

| |
|---|
| **The CSTARS accepts data from Government systems, and supplements this data for acquisition management for services, goods, or materials provided by the vendor community to the Federal Government.** |

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 information. Information system security controls used to protect this information are implemented, validated, and continuously monitored. NIST user access is restricted to authorized users and risk is minimized through limiting the number of authorized users.**<br><br>**In addition, NIST requires and has in place:**<br><br>• **Staff mandatory annual IT Security Training requirements.**<br>• **Annual renewal of IT security Rules of Behavior for NIST staff.**<br>• **Policies and procedures for storage and disposal of sensitive electronic data.**<br>• **System data encryption at rest and in transit.** |

## 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 - Federal agencies** |
| **Case-by-Case - DOC bureaus** |
| **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: |
|---|
| **The CSTARS connects with or receives information from the following information systems:**<br>• **General Services Administration Federal Procurement Data System - Next Generation (FPDS-NG); transmission of data to this application from CSTARS is via TLS encrypted sessions**<br>• **General Services Administration System for Award Management (SAM); data received from SAM is via SFTP/SSH and stored on secure servers within the NIST protected network.**<br>• **General Services Administration System Federal Business Opportunities (FedBizOpps); data sent or received to this system is via TLS encrypted sessions.**<br>• **Office of Management and Budget MAX, Department of Commerce Acquisition Data Warehouse; transmission of data to this application is via SFTP/SSH connections**<br>• **NOAA1101, Information Technology Center (ITC) General Support System (GSS) Commerce Business System component; transmission of data to this application is a via point-to-point Virtual Private Network (VPN) over the Internet.**<br>• **NIST 162-01, Commerce Business System, Core Financial System (CBS/CFS); data is transmitted over internal NIST network in a firewall protected zone. Data on the CBS/CFS is encrypted at rest and in transit.**<br>• **NIST 188-01 Platform Services Division (ServiceNow) – There are two fields exported to ServiceNow via SFTP/SSH which are considered 'Procurement Sensitive' fields, but no PII/BII is transferred.** |

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

| Class of Users |
|---|
| **Government Employees**<br>**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 by other means.** |
|---|
| The Privacy Act statement and/or privacy policy can be found at: |
| |
| The reason why notice is/is not provided: |
| **Individuals are notified if their PII/BII is collected, maintained, or disseminated through the GSA SAM registration process.** |

7.2 Indicate whether and how 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: |
| **Individuals do have the opportunity to decline providing PII/BII with GSA SAM. However, doing so may result in not doing business with the Federal Government.** |

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: |
| **Individuals do have the opportunity to consent to particular uses of their PII/BII when registering with GSA SAM.** |

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

| No, individuals do not have an opportunity to review/update PII/BII pertaining to them. |
|---|
| The reason why individuals can/cannot review/update PII/BII: |
| **Vendors do have an opportunity to review and update their profiles within GSA SAM.** |

## 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.**<br><br>**Staff (employees and contractors) received training on privacy and confidentiality policies and practices.**<br><br>**Access to the PII/BII is restricted to authorized personnel only.**<br><br>**Access to the PII/BII is being monitored, tracked, or recorded.**<br><br>**The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements.**<br><br>**The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.**<br><br>**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).**<br><br>**A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.**<br><br>**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.** |
| The information is secured in accordance with FISMA requirements. |

| |
|---|
| **Is this a new system? No**<br>**Below is the date of the most recent Assessment and Authorization (A&A).**<br>**10/15/2019** |
| 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 application is 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. Data on the servers is encrypted at rest and in transit.**<br><br>**For information sharing, PII is transferred in a secure fashion. 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. Access to CSTARS requires NIST-issued credentials because access is restricted by user authentication. NIST remote and other agency users access CSTARS on an authorized DOC network, or via connecting to the NIST network through a Virtual Private Network (VPN).** |

## 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: |
| **GSA/GOVT-6, GSA SmartPay Purchase Charge Card Program**<br>**GSA/GOVT-9, System for Award Management (SAM)**<br>**GSA/GOVT-10, Federal Acquisition Regulation (FAR) Data Collection 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 1.1 Financial Management and Reporting Records |
|---|
| The stage in which the project is in developing and submitting a records control schedule: |
| |
| **No, retention is not monitored for compliance to the schedule.** |
| Reason why retention is not monitored for compliance to the schedule: |
| **The CSTARS does not have the technical capability to archive/purge records.** |

10.2 Indicate the disposal method of the PII/BII.

| Disposal |
|---|
| **Shredding** |
| **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 |
|---|---|
| **Quantity of PII**<br>**Context of Use**<br>**Obligation to Protect Confidentiality** | **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.**<br><br>**Context of Use- The purpose for which the information is collected supports the administrative business of NIST.**<br><br>**Obligation to Protect Confidentiality- The organization is legally obligated to protect the personal and business identifiable information within the acquisition application. The loss of confidentiality in the form of proprietary business information and other financial information, which if disclosed to unauthorized sources, could cause unfair advantage for vendors, contractors, or individuals and could result in financial loss or adverse legal action against NIST.** |

## 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.)

| |
|---|
| **CSTARS does not collect data from individuals. The use of SAM, FPDS-NG, FEDBizops, and OMB Max are required per Federal Acquisition Regulations and other Federal and DOC acquisition/procurement policies. Only data required for the acquisition of services and material/products from vendors (commercial and government) and reporting these purchases is used in the CSTARS application. Training and rules of behavior can raise the necessary awareness to mitigate data mishandling.** |

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 |
| |