

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



**Privacy Impact Assessment
for the
138-01 Business Operations Office (BOO) System**

Reviewed by: Claire W. Barrett

- Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
 Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

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: 138-01

Introduction: System Description

Provide a brief description of the information system:

The NIST Business Operations Office (BOO) system is used to implement an enterprise-level Customer Relationship Management (CRM) system so that NIST organizations can manage interactions and relationships with customers while also offering an online storefront to sell NIST products and services to the public.

The Salesforce application is owned by the Business Operations Office (BOO) which is part of Management Resources organization at NIST. Implementation of Salesforce is the responsibility of NIST 188-01 – Platform Services Division. The various OUs that use Salesforce own the data associated with the respective implementations.

Portions of this PIA have been updated to address the addition of the Creating Helpful Incentives to Produce Semiconductors and Science (CHIPS) Salesforce Cloud (CSfC) environment to the existing 138-01 BOO System. Editorial and formatting changes have also been made to ease reading of the document. The reader is recommended to review the document in its entirety to develop a comprehensive understanding of NIST’s privacy program with regards to the collection and use of information in support of CHIPS.

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

This is a general support system.

b. System location

On premise portions of the system are located at the NIST facility in Gaithersburg, MD while the cloud-based components are managed in the Salesforce Government Cloud+.

CSfC operates exclusively in the Salesforce Government Cloud+ and does not have on-premises components.

c. Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

System interconnects with NIST 188-01, NIST 162-01, and NIST 640-01.

The CSfC is a standalone environment and does not connect with any external systems. It interconnects with NIST 181-04, Network Infrastructure which provides IT security services for NIST operations as well as NIST 188-01, Platform Services Division which provides application support.

d. The way the system operates to achieve the purpose(s) identified in Section 4

BOO's vision is to fulfill its mission to deliver exceptional products and services using project management, process engineering, relationship management, and customer engagement as follows:

CRM - BOO works with stakeholders across NIST to provide an enhanced understanding of how NIST interacts with customers and partners.

The CRM system will provide NIST with customer and business information about how NIST provides products, services and any related inquiries. CRM data will be collected and entered by NIST OU users and will contain customer PII and BII. This instance (<https://nist.my.salesforce.com>) also contains a Maintenance and Operation module which is used by the NIST CRM vendor to provide helpdesk support to NIST users.

Information is obtained by the public who are reaching out to NIST for NIST products and service. All data is non-sensitive customer email and contact information copied by NIST staff from Microsoft Office 365 or entered via a public facing form (<https://www.nist.gov/about-nist/contact-us>).

E-Commerce - BOO leads the effort to improve how NIST transactions take place. They do this by implementing and managing an e-commerce platform that allows customers to place online orders while they manage invoice and payment processes.

E-Commerce includes a web-based storefront (<https://shop.nist.gov>) that allows customers to view and purchase products in the NIST catalog. After creating an account, customers can make purchases, retrieve order history, status, invoices/receipts, and self-service their data and passwords. User account data includes customers name, address, and e-mail. Customers can pay for services using checks, wire transfers, purchase orders, Intra-governmental Payment and Collection (IPAC), and the Pay.gov payment service. The storefront has been customized for NIST, and information is generated in the cloud.

E-Commerce will also use an externally hosted application, DocuSign. The application will be used to obtain signatures from both internal NIST users as well as external customers. Signatures will be generated on various product and service reports, distributor agreements, and site license orders as well as NIST return shipping forms (NIST 64). These services will be used by Calibrations, Standard Reference Data (SRD), Standard Reference Materials (SRM), and Standard Reference Instruments (SRI).

CSfC - consists of the following components:

- CHIPS Inquiry Management
 - Email inquiries: Members of the public may send inquiries regarding the CHIPS program to one of two mailboxes; general inquiries are submitted to askchips@chips.gov; and questions specific to incentive applications are sent to apply@chips.gov. Email inquiries are managed in a customer care queue and responses are provided by email.
 - Engagements and Meetings: is a public facing online form (AskCHIPS - <https://askchips.chips.gov>) through which members of the public may request . The form captures the desired engagement type (e.g., meeting, keynote, webinar,

etc.) and as well as relevant details for the request (e.g., preferred date, location, expected discussion topics, requested speakers, etc.).

- CHIPS Incentives Portal (CHIPS Portal) is a public facing environment (<https://applications.chips.gov>) that supports the management of required information from semiconductor organizations interested in the CHIPS incentives program. Semiconductor organizations (applicants) establish an account in the system to manage their organization's submissions and provide NIST with a point of contact and contact information for any follow-up communications. The CHIPS Portal consists of the following applications:
 - Statement of Interest (SOI): Used by potential applicants to provide preliminary business proposal/project specific data. Some of this information (organization name, point of contact, etc.) may be used to pre-populate Pre-Applications and/or Application for incentives. NIST uses the SOI to understand the potential incentives request pipeline, and plan staffing and other supports for applications likely to be submitted in the future.
 - Pre-Application: Used by potential applicants to submit the optional pre-application and associated documents. NIST uses Pre-Application information to provide feedback to potential applicants, improve the quality of the applications, and further plan for incoming application processing.
 - Application: Used by applicants to submit formal applications for the CHIPS Incentives program. NIST uses Application information to make incentive award decisions.
 - All records created and submitted in the CHIPS Portal by the applicant are part of the applicant record and not that of the individual filing the submission or the point-of-contact named in the applicant files. NIST uses the point-of-contact information to engage with the Applicant on matters pertaining to the technical submission only.

e. How information in the system is retrieved by the user

CRM data is accessed directly through the component by authorized NIST users. Role-based permissions are used.

E-Commerce data is also accessed directly through the component via navigation from nist.gov or shop.nist.gov URLs. Then after customers have created an account, they can sign in to make a purchase. When a customer creates an account, they will enter name, address, and email which will be generated in the Salesforce cloud. Once they have an account, they will be able to retrieve their order history, status, invoices/receipts, and self-service their data and passwords. Internal NIST end users who support the customers on this system must access the backend system behind the NIST firewall and access must go through the SSO.

After a customer places an order within the system, administrators fulfill the order and prepare for shipping. Customers will then receive an email with a link to download the products. E-Commerce customer service agents use an internal portal to manage customer orders and to provide customer service.

CHIPS Inquiry Management: once submitted, inquiries cannot be retrieved by the submitter. Authorized NIST users retrieve records by the autogenerated customer care queue ID or the submitter's email address. Each inquiry submission results in the creation of a unique customer care queue ID.

CHIPS Portal: Applicants may access their records inside the portal at any time using the organizational account created with the initial submission. Typically, this account is created at the SOI phase, but may be created at the Pre-Application or Application phases. NIST authorized users of the CHIPS Portal retrieve Applicant records by the applicant name through a secure backend system.

f. How information is transmitted to and from the system

All system connectivity is via TCP/IP across the NIST Network Infrastructure (SSP 181-04). The NIST Network Infrastructure system provides all services for physical cabling, network frame synchronization/ flow control/ error checking, routing, switching, and DNS.

Remote connections to NIST internal resources are made via SSL Remote Access services managed as part of the NIST Network Security system (SSP 181-01).

g. Any information sharing conducted by the system

E-Commerce has integrations with other entities and third-party systems to carry out specific functions to complete and record customer transactions. These include:

1. Pay.Gov (Treasury) – Salesforce submits order details to Pay.gov to process electronic credit card payments via webservices. E-Commerce uses Hosted Collection Pages Service (HCPS), which is part of Trusted Computing Services suite. E-Commerce does not store or track customer payment information.
2. Commerce Business System/Commerce Financial System (NIST 162-01) - Accounts receivable files and billing invoice files are produced from Salesforce B2B and manually downloaded from the Salesforce Cloud. Files are then saved onto a user's secure network, and then uploaded to the CBS database server via chron job. Payment transactions are also provided by Treasury to be uploaded to CBS, but this activity takes place outside of the Salesforce environment.
3. DocuSign – Used to obtain electronic signatures from customers as well as NIST users on various reports generated through the NIST storefront.
4. Limestone application (NIST 640-01) - An internal web-based application to generate the PDFs required for customers such as invoices, quotes, and receipts. In Phase 1, Limestone will generate: perform invoice, quote, and receipt. Phase 2 will expand this feature.
5. NIST does not provide access to the CSfC to any other system and only authorized CHIPS staff may access the records in the 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 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.

The CSfC supports implementation of the of the Creating Helpful Incentives to Produce Semiconductors and Science Act of 2022 (CHIPS Act), August 9, 2022.

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

The non-CSfC portion of the system is Moderate. However, the FIPS security impact category for the CSfC is High.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

This is an existing information system in which changes that create new privacy risks.

- New Interagency Uses: The CsfC is a new component within the previously approved NIST 138-01 BOO system. The personally identifiable information (PII) collected and maintained in the CSfC is not materially different than the types of PII already in the system, as such the privacy risk of the system has not changed.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated.

General Personal Data (GPD)

- Name
- Home Address (not collected through CSfC components)
- Telephone Number (not collected through CSfC components)
- Email Address (may be collected if members of the general public initiate an inquiry through CHIPS Inquiry Management processes)

Work-Related Data (WRD)

- Occupation
- Job Title
- Work Address
- Work Telephone Number
- Work Email Address
- Business Associates
- Proprietary or Business Information
- Resumes of individuals working for CHIPS applicants (these records are part of the Application file and are not retrieved by identifiers linked to the individual)

System Administration/Audit Data (SAAD)

- User ID
- IP Address
- Date/Time of Access

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*

*Members of the public who engage with CHIPS using one of the Inquiry CHIPS Management processes, furnish their name and email address directly. Records in the customer care queue may be supplemented with information provided to NIST during inquiry communications. Information is entered in the record by NIST staff.

Information necessary to establish an account in the CHIPS Portal is collected directly from the individual establishing the account on behalf of the applicant. Point-of-contact information collected in SOI/Pre-Application/Application may not be the same as that of the individual accessing the portal on behalf of the Applicant and therefore may not be collected directly from them.

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

Accuracy is ensured in CRM because data is collected directly from the user. If data needs to be corrected or updated, an individual may contact their NIST point of contact.

The NIST Storefront collects customer data directly from users (i.e., public customers), and users can review/update their profile through the online portal at any time. Data is also reviewed by NIST staff to ensure fulfillment of the order. Once completed, the orders are then sent to either Pay.gov or NIST 162- 01 for payment. Notifications will be sent to users to confirm successful payment.

If a signature is required for a transaction, signatures and documents are uploaded, encrypted, and a unique hash is created. If a signed document has been tampered with or compromised, the hash will not match the Digital signature information.

Accuracy is ensured in CSfC because data is collected directly from the parties submitting forms, emails, or incentive application packages.

NIST 188-01 infrastructure maintains controls (e.g., encryption at rest and encryption in transit) to ensure the data cannot be altered by unauthorized persons.

2.4 Is the information covered by the Paperwork Reduction Act?

The following information collection requests (ICR) are associated with CSfC functions:

- Inquiry Management/Engagement and Meeting Requests - 0693-0092.
- CHIPS Portal/SOI - 0693-0091
- CHIPS Portal/Pre-Application – ICR number will be added to collection instrument once assigned by the Office of Management and Budget (OMB)
- CHIP Portal/Application – ICR number will be added to collection instrument once assigned by OMB

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed.

N/A

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns.

N/A

Section 4: Purpose of the System

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

- For administrative matters
- To improve Federal services online
- For employee and customer satisfaction

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

CRM: Business contact information will be used to better integrate and communicate with various business communities. CRM enables NIST 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. In turn, NIST is able to better understand customer needs. CRM also allows NIST to automate its workflows, allowing insight into the status of Cooperative Research and Development Agreements (CRADAs). The PII/BII in the CRM may be about federal employees, federal contractors, foreign nationals, members of the public, or partners and stakeholders.

E-Commerce: Scientific and technology related sales take place via the E-Commerce component, and PII is be used to facilitate that process.

The redress of customer's information will be mostly self-serviced by the customer. Additionally, contact information (names/emails/phone numbers) will be provided for

customers to directly contact someone at NIST to update their information if they run into a problem or have a request they cannot perform themselves.

CHIPS Inquiry Management/Email: NIST uses contact information to respond to inquiries about the CHIPS program, the CHIPS incentives process, and requests to meet with CHIPS officials
 CHIPS Portal: NIST uses information in the SOI to understand the potential incentives request pipeline, and plan staffing and other supports for applications likely to be submitted in the future. Pre-Application information is used to provide feedback to potential applicants, improve the quality of the applications, and further plan for incoming application processing. Application information is used to make incentive award decisions and inform applicants of application outcomes.

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.)

CRM: Salesforce has an approval process used before sharing data. Salesforce also takes advantage of contractual clauses and Rules of Behavior. Cloud activity can mean some limited risk.

E-Commerce: Activity does not present significant risk and has its own Rules of Behavior form for internal users to sign before obtaining access.

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 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared.

NIST may share non-CHIPS related PII/BII in the IT system in the following manner:

- Within the bureau - Bulk Transfer, Case-by-Case*, Direct Access **
- Federal Agencies - Case-by-Case**

* Case-by-Case – Within the Bureau (NIST 162-01 used for payments), and Direct Access – Within the Bureau (NIST 188-01 for platform services, NIST 640-01 for use of Limestone)

** Case-by-Case - Federal Agencies – (Treasury (pay.gov) used for payments)

The CSfC contains information submitted in response to CHIPS Incentive Program – Notice of Funding Opportunities (NOFOs). As noted in Section IV.C.3 of the CHIPS Incentive Program – Commercial Fabrication Facilities Notice of Funding Opportunity (NOFO), information and data contained in or submitted in connection with statements of interest, pre-applications, full applications, or due diligence under this NOFO (together, “applicant information and data”) may be accessed and used by Federal employees for the purposes of the Notice of Funding Opportunity (NOFO) and carrying out the government’s responsibilities in connection with the CHIPS Incentives Program, or as otherwise required by law.

6.2 *Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?*

No, the external agency/entity is not required to verify with the NIST before re-dissemination of PII/BII.

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

The non-CSfC portion of the 138-01 BOO System connects with or receives information the following IT system(s) authorized to process PII and/or BII.

- NIST 188-01, Platform Services Division (PSD)
- NIST 162-01, Commerce Business System, Core Financial System (CBS/CFS)
- NIST 640-01, Office of Reference Materials (ORM) System
- Pay.gov
- The CSfC connects with NIST 188-01, Platform Services Division for the purposes of system management, and utilizes the 181-04, Network Infrastructure.
- Technical controls for all system connections are described in Section 8.2.

6.4 *Identify the class of users who will have access to the IT system and the PII/BII.*
Class of Users

- Government Employees
- Contractors
- General Public *
- Other **

*Customers from the general public will have access to the NIST Storefront portal but will only be able to access their own account information.

**Individuals who use the CHIPS Inquiry Management solutions will not have access to the system. Applicants who create accounts in the CHIPS portal will have access their own account information and records.

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 general NIST Privacy Act Statement and/or privacy policy can be found at <https://www.nist.gov/privacy-policy>.
 - E-Commerce: A Privacy Act Statement is found on customer registration profile pages: https://shop.nist.gov/ccrzCCSiteRegister?cartId=&portalUser=&store=&cclcl=en_US (see Appendix A)
- Yes, notice is provided by other means.
 - CRM: Notice is provided on the web form interface where inquiries are received by the public. It is recommended that notice is provided verbally when obtaining information in person.
 - E-Commerce: The Privacy Act Statement is also presented in the shopping cart after selection of a product.
 - CHIPS Inquiry Management/Engagement and Meetings: The general NIST Privacy Policy is provided on web pages directing users to the CHIPS inquiry email. It is recommended that notice be provided verbally when obtaining information in person.
 - CHIPS Inquiry Management/Engagement and Meetings: A Privacy Act statement is included on the web form.

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

CRM: Individuals have the opportunity to decline to provide PII/BII 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/or conduct business with NIST.

E-Commerce: 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.

CHIPS Inquiry Management: individuals may decline to provide PII/BII by not submitting an inquiry email or completing the AskCHIPS webform.

CHIPS Portal: Applicants may decline registering in the portal or providing contact information for a point of contact. In doing so, they will not be able to submit SOIs, Pre-Applications, or Applications for CHIPS incentives.

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

CRM: Opportunity to consent to particular uses of PII/BII is provided on the web form interface where inquiries are received by the public. It is recommended that notice is provided verbally when obtaining the information in person.

E-Commerce: Customers have the ability to consent to particular uses of their individual profile information upon registration.

CSfC: NIST notifies of the need for and use of PII/BII prior to submission. NIST limits the use of the data through technical, administrative, and physical controls for the purposes for

which it was collected and authorized by law.

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

CRM: Opportunity to review/update PII/BII 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> .

E-Commerce: Customers have the ability to review/update their profile information at any time through the NIST storefront.

CHIPS/Inquiry Management: Information provided through the inquiry management tools may be updated through the submission of an additional inquiry or by responding to follow-up communications from NIST.

CHIPS Portal: Information provided through the Portal may be reviewed and/or updated by accessing the applicant account and modifying the account registration information, SOI, Pre-Application, or Application.

Section 8: Administrative and Technological Controls

8.1 *Indicate the administrative and technological controls for the system.*

The following statements apply to all NIST 138-01 BOO System components:

- 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 5 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.

- Access controls are in place as role-based permissions are used
- The most recent Assessment and Authorization (A&A) for this system is 04/30/2022

8.2 ***Provide a general description of the technologies used to protect PII/BII on the IT system.***

The following statements apply to all NIST 138-01 BOO System components:

- Unauthorized use of the system is restricted by user authentication, account management processes, and segregation of privileged user accounts and devices. Access logs are also 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, or FIPS NIST 140-2 encrypted virtual private network technologies between organizations and the public. Access to the administrative interface is limited to hardware using a NIST IP address, combined with user authentication (NIST-issued credentials).
- All system connectivity is via TCP/IP across the NIST Network Infrastructure (SSP 181-04). The NIST Network Infrastructure system provides all services for physical cabling, network frame synchronization/flow control/error checking, routing, switching, and DNS.
- Remote connections to NIST internal resources (i.e., telecommuting, travel, etc.) are made via SSL Remote Access services managed as part of the NIST Network Security system (SSP 181-01).

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. 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.”***

Records in the system are covered by the following system of records notices (SORN).

CRM/E-Commerce

- [DEPT-2, Accounts Receivable 68 FR 35849](#)
- [DEPT-23, Information Collected Electronically in Connection with Department of Commerce Activities, Events, and Programs 78 FR 42038](#)

CHIPS Inquiry Management:

- [DEPT-10, Executive Correspondence Files 79 FR 72623](#)

Section 10: Retention of Information

10.1 *Indicate whether these records are covered by an approved records control schedule and monitored for compliance.*

The following apply to non-CSfC records maintained in the system

- [GRS 5.1/020](#) Non-recordkeeping copies of electronic records
- [GRS 5.2/020](#) Intermediary Records
- [GRS 6.5/010](#) Public customer service operations records
- [GRS 6.5/020](#) Customer/client records
- Note that information inputted into the CRM component from other information systems is referential and thus defers to the originating source of input to control the records.
- Retention is monitored for compliance to the schedule.

The following apply to records maintained in the CSfC

- [GRS 1.2/020](#) Grant and cooperative agreement case files
- [GRS 5.1/020](#) Non-recordkeeping copies of electronic records
- [GRS 5.2/020](#) Intermediary Records
- [GRS 6.5/010](#) Public customer service operations records
- [GRS 6.5/020](#) Customer/client records
- Retention is monitored for compliance to the schedule.

10.2 *Indicate the disposal method of the PII/BII.*

- Records are disposed of via shredding and deleting.

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.*

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

11.2 *Indicate which factors were used to determine the above PII confidentiality impact level.*

The following apply to all PII maintained in the system:

- Identifiability: The data types that are collected and maintained can be used to identify specific individuals.
- Quantity of PII: The quantity of the PII that is collected and maintained pertains to members of the public.
- The volume of data transmitted that may include other personally identifiable information is unknown.
- Context of Use: Customers providing information to obtain a product or service.
- Obligation to Protect Confidentiality: The organization is legally obligated to protect the PII within the applications.
- Access to and Location of PII: The data is stored in the cloud.

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.***

- 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.
- Threats could arise from having multiple storefronts and subsequently multiple systems to transact E- Commerce. NIST centralized its E- Commerce systems into a single system to ensure consistency with management, administration, and technical controls.
- A risk exists with authorized users entering inaccurate information into the CRM and the CHIPS Inquiry Management components. This risk is mitigated through internal user training. A risk also exists with the general public entering incorrect information into the E-Commerce and CHIPS Inquiry Management 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 use of NIST 162-01 CBS/CFS and Pay.gov services eliminates the need to process and store user's information in the BOO system, reducing risk associated with user's 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 required business process changes.

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.

Appendix A – Privacy Act Statement for E-Commerce

 Shop NIST | E-Commerce Store × +

 https://shop.nist.gov/ccrz_CCISiteRegister?cartId=&portalUser=&store=&ccid=en_US

PRIVACY ACT STATEMENT

- 1. Authority:** The collection of this information is authorized under 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-Wylder Technology Innovation Act of 1980, as amended, 15 U.S.C. 3710a.; 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.
- 2. Purpose:** NIST is collecting this information to permit the inventory, order, and purchase of materials and informatic reference materials by the public. Subsequent payment information may be collected to enable supporting financial activities (e.g., invoicing, tracking, payment). Information regarding the purchase is tracked for programmatic and mission activities (e.g., supply/demand, communities who purchase, etc.).
- 3. Routine Uses:** NIST will use this information to process product transactions (which may include relaying updates as to status of shipment, and/or updates regarding products). *Disclosure of this information is permitted under the Privacy Act of 1974 (5 U.S.C. Section 552a) to be shared among Department staff for work-related purposes. Disclosure of this information is also subject to all of the published routine uses as identified in the Privacy Act System of Records Notice [COMMERCE/DEPT-2](#) and [COMMERCE/DEPT-23](#).*
- 4. Disclosure:** Furnishing this information is voluntary. However, this information is required in order to proceed with a purchase. The failure to provide accurate information may result in the requested item not arriving to the purchased destination successfully. The failure to provide accurate information may also delay or prevent you from receiving the product. Submitting voluntary information constitutes your consent to the use of the information for the stated purpose. When you submit the information, you are indicating your voluntary consent for NIST to use of the information you submit for the purposes stated, and shared with other internal systems.

NIST will protect from unauthorized disclosure personally identifiable information or business identifiable information that is submitted to NIST on this site. Federal law or regulation may require disclosure under limited circumstances. This information may be retained indefinitely as deemed necessary for the purpose of distributing updates and information. For additional information, see the NIST Privacy Policy.

Points of Contact and Signatures

<p>Information System Security Officer or System Owner</p> <p>Name: Zhang, Yali Office: 101/A0435 Phone: 301-975-2345 Email: yali.zhang@nist.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature: <u>YALI ZHANG</u> Digitally signed by YALI ZHANG Date: 2023.03.22 09:55:49 -04'00'</p> <p>Date signed: _____</p>	<p>Chief Information Security Officer</p> <p>Name: Heiserman, Blair Office: 225/A115 Phone: 301-975-3667 Email: nist-itso@nist.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature: <u>Blair Heiserman</u> Digitally signed by BLAIR HEISERMAN Date: 2023.03.22 11:50:04 -04'00'</p> <p>Date signed: _____</p>
<p>Co-Authorizing Official</p> <p>Name: Vanek, Anita Office: 101/A1124 Phone: 301-975-3744 Email: anita.vanek@nist.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature: <u>ANITA VANEK</u> Digitally signed by ANITA VANEK Date: 2023.03.22 09:41:34 -04'00'</p> <p>Date signed: _____</p>	<p>Authorizing Official</p> <p>Name: Sastry, Chandan Office: 225/B222 Phone: 301-975-6500 Email: chandan.sastry@nist.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature: <u>CHANDAN SASTRY</u> Digitally signed by CHANDAN SASTRY Date: 2023.03.21 15:27:31 -04'00'</p> <p>Date signed: _____</p>
<p>Privacy Act Officer</p> <p>Name: Fletcher, Catherine Office: 101/A523 Phone: 301-975-4054 Email: catherine.fletcher@nist.gov</p> <p>I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA.</p> <p>Signature: <u>CATHERINE FLETCHER</u> Digitally signed by CATHERINE FLETCHER Date: 2023.03.22 11:13:27 -04'00'</p> <p>Date signed: _____</p>	<p>Chief Privacy Officer</p> <p>Name: Barrett, Claire Office: 225/B226 Phone: 301-975-2852 Email: claire.barrett@nist.gov</p> <p>I certify that the PII/BII processed in this IT system is necessary and this PIA ensures compliance with DOC policy to protect privacy.</p> <p>Signature: <u>CLAIRE BARRETT</u> Digitally signed by CLAIRE BARRETT Date: 2023.03.21 14:53:31 -04'00'</p> <p>Date signed: _____</p>

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.