Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
201-01 CHIPS Program Office 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

CHARLES CUTSHALL Digitally signed by CHARLES CUTSHALL
Date: 2023.12.22 14:52:46 -05'00' 12/19/2023

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: 201-01

Introduction: System Description

(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
(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

Provide a brief description of the information system:
The 201-01 CHIPS[1] Program Office (CPO) System supports NIST with implementation of the CHIPS and Science Act to strengthen and revitalize the U.S. position in semiconductor research, development, and manufacturing, while investing in American workers. The CHIPS Program Office provides incentives for investment in facilities and equipment in the United States.

The following system component contains or otherwise stores, processes, or transmits sensitive PII and/or BII:

- **Cloud-Salesforce for CHIPS (CSfC) includes multiple subcomponents:**
  - **CHIPS Inquiry Management**
  - **CHIPS Incentives Portal (i.e., CHIPS Portal)**

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

The CSfC is part of the 201-01 CHIPS Program Office System, which is a general support system.

b. System location

The CSfC operates in the Salesforce Government Cloud Plus and does not have on-premises subcomponents.

[1] Creating Helpful Incentives to Produce Semiconductors (CHIPS)

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

The CSfC is a standalone environment, receiving information from the General Services Administration's (GSA's) System for Award Management (SAM).

The CSfC relies on the 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*

The CSfC consists of the following subcomponents:

- **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; 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 information. The form captures the desired engagement type (e.g., meeting, keynote, webinar, etc.), 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. The CHIPS Portal consists of the following:
  - *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, plan staffing, and other support.
  - *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 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.

- *CHIPS Incentives 4.2 Mulesoft SAM.gov:* Consists of a Mulesoft Integrator that interconnects the Salesforce Government Cloud Plus environment with the General Services Administration's (GSA's) System for Award Management (SAM). NIST staff validate participating CHIPS application entities (businesses) with SAM.gov using the applicant provided Unique Entity Identifier (UEI), generated when an entity registers with SAM.gov.
- *CHIPS Transaction Advisor Portal:* Enables functionality to manage and track role-based access to third-party organizations when asked to review CHIPS Incentives applications. The third-party organizations require establishment of a Cooperative Research and Development Agreement (CRADA) before access is granted based on need.

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

Information in the CSfC is retrieved as follows:

- **CHIPS Inquiry Management:** Authorized staff 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. The submitter cannot retrieve their inquiry once submitted.
- **CHIPS Portal:** Authorized staff retrieve Applicant records by the Applicant (i.e., entity/organization) name through a secure backend system. Applicants may access their records inside the Portal at any time using the organizational account created with the initial submission (created at either SOI, Pre-Application, or Application phases).

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

Information in the CSfC is transmitted in the following manner:

- **CHIPS Inquiry Management:** Email askchips@chips.gov; Email apply@chips.gov for questions specific to incentive applications; directly in public facing online (AskCHIPS - https://askchips.chips.gov)
- **CHIPS Portal:** Directly in the public facing Portal (https://applications.chips.gov)

All system connectivity is via TCP/IP across the NIST 181-04, Network Infrastructure System. 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 181-01, Network Security System.

g. *Any information sharing*

The CHIPS Incentives Program is authorized by the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (P.L.116-283), as amended by the CHIPS and Science Act of 2022 (P.L. 117-167) (the "CHIPS Act"). 15 U.S.C. § 4652. The CHIPS Act establishes the confidentiality of records submitted by a "covered entity" pursuant to the CHIPS Incentives Program (15 U.S.C. § 4652). Except for information "relevant to any administrative or judicial action or

proceeding," "that a covered entity has consented to be disclosed to third parties," or "necessary to fulfill [certain] congressional notification" requirements under the statute, "any information derived from records or necessary information disclosed by a covered entity to the Secretary" is exempt from disclosure under FOIA and "shall not be made public." 15 U.S.C. § 4652(a)(6)(G). This policy protects the confidentiality of such information pursuant to the CHIPS Act and consistent with other relevant statutes, including the Freedom of Information Act, 5 U.S.C. § 552, and the Trade Secrets Act, 18 U.S.C. § 1905.

For additional information on how NIST's Handling of Confidential Information, please see the CHIPS program website at (https://www.nist.gov/chips/handling-confidential-information).

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 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

High

Section 1: Status of the Information System

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

This is a new information system in which changes create new privacy risks.

Changes That Create New Privacy Risks (CTCNPR)
New System/System Management Change: This system was created to support the CHIPS Program Office. Limited application development was previously authorized under NIST System 138-01, initially leveraging the existing NIST Salesforce operating environment. The environment has since been segregated into an operating environment for the sole use of the CHIPS Program Office. To keep pace with programmatic needs, iterations of development have occurred and authorization to operate obtained for each iteration. This new system includes the new CSfC operating environment and each iteration of development, to date, with limited privacy risk.
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. *(Check all that apply.)*

Identifying Numbers (IN)

Other*
Other identifying numbers:
***Unique Entity Identifier (UEI) for the CHIPS Incentives Applicant. The UEI is not assigned to an individual.** **Consolidation Key (if an applicant is applying as part of a consortium)**
Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:

General Personal Data (GPD)
Name **Email Address (may be collected if members of the general public initiate an inquiry through CHIPS Inquiry Management processes)**
Other general personal data:

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 an individual)**
Other work-related data:

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. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains
In Person **Telephone** **Hard Copy – Mail/Fax** **Email** **Online** **Other***

Other:
***Members of the public who engage using one of the CHIPS Inquiry 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.**

Government Sources
Other:

Non-government Sources
Other:

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

Accuracy is ensured in CSfC because data is collected directly from the party submitting forms, emails, or Incentive applications.

NIST 181-04, Network Infrastructure System, NIST 181-01, Network Security System, and NIST 188-01, Platform Services Division provide and maintain the infrastructure controls and system administration (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?

Yes

The OMB control number and the agency number for the collection:

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

- **CHIPS Inquiry Management (Email Inquiries/Engagement and Meeting Requests) - 0693-0092**
- **CHIPS Portal/SOI - 0693-0091**
- **CHIPS Portal/Pre-Application – 0693-0095**
- **CHIPS Portal/Application – 0693-0094**
- **CHIPS Streamline Supply Chain 0693-0097**
- **CHIPS Environmental Questionnaire 0693-0093**
- **CHIPS Recipient Reporting – pending approval**
- **CHIPS National Environmental Policy Act (NEPA) Financial Disclosures – pending approval**
- **CHIPS Research and Development (R&D)* – pending approval**

***R&D activities covered by this PRA package are within the CPO.**

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)

N/A
Other:

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

The IT system supported activities which raise privacy risks/concerns.

Activities
N/A
Other:

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose
For administrative matters **To improve Federal services online** **For employee and customer satisfaction**
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 PII/BII identified in Section 2.1 is in reference to a member of the public (e.g., organizational Applicant or individual with an inquiry/engagement request).

CHIPS Inquiry Management: 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 resources. 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.)

Information collected is directly from the individuals or Applicant POC and is limited to only that which is needed for the service. **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).** **Mitigating controls include employing and monitoring 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. *(Check all that apply.)*

NIST may share PII/BII in the IT system in the following manner:

- **Within the bureau – Case-by-Case; Direct Access**
- **DOC bureaus – Case-by-Case**
- **Federal agencies – Case-by-Case**
- **Other– Case-by-Case (see response below)**

The recipients the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared.

The CHIPS Incentives Program is authorized by the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (P.L.116-283), as amended by the CHIPS and Science Act of 2022 (P.L. 117-167) (the "CHIPS Act"). 15 U.S.C. § 4652. The CHIPS Act establishes the confidentiality of records submitted by a "covered entity" pursuant to the CHIPS Incentives Program (15 U.S.C. § 4652). Except for information "relevant to any administrative or judicial action or proceeding," "that a covered entity has consented to be disclosed to third parties," or "necessary to fulfill [certain] congressional notification" requirements under the statute, "any information derived from records or necessary information disclosed by a covered entity to the Secretary" is exempt from disclosure under FOIA and "shall not be made public." 15 U.S.C. § 4652(a)(6)(G). This policy protects the confidentiality of such information pursuant to the CHIPS Act and consistent with other relevant statutes, including the Freedom of Information Act, 5 U.S.C. § 552, and the Trade Secrets Act, 18 U.S.C. § 1905. **For additional information on how NIST's Handling of Confidential Information, please see the CHIPS program website at (https://www.nist.gov/chips/hading-confidential-information).**
Other:

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

The CPO may share some Application Information and Data with other Federal agencies. Such sharing will be justified by a programmatic purpose, done only on a need-to-know basis, and in the cases of systematic sharing, will be governed by interagency agreements or other agreed-upon protocols. Exceptions to this requirement may include cases where the sharing is carried out by authorized redisclosure personnel (e.g. in a briefing in aggregated or abbreviated form). Other rare exceptions may apply at the discretion of the CPO Director and Chief Counsel for Semiconductor Incentives.

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

Yes
The name of the IT system and description of the technical controls which prevent PII/BII leakage:
NIST 188-01, Platform Services System **NIST 181-04, NIST Network Infrastructure System** **NIST 181-01, NIST Network Security System** **General Services Administration's (GSA's) System for Award Management (SAM)** **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. *(Check all that apply.)*

Class of Users
Government Employees **Contractors (to include authorized NIST Associates and third party reviewers)** **General Public** **Other ***
Other:
***Individuals who use the CHIPS Inquiry Management do not have access to records in the system. Applicants who create accounts in the CHIPS Portal will have access to 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.** **Yes, notice is provided by other means.** • **CHIPS Inquiry Management: 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. A Privacy Act statement is included on the AskCHIPS web form.** • **CHIPS Portal: The general NIST Site Privacy Policy is provided on web pages in the Portal.**
The Privacy Act Statement and/or privacy policy can be found at:
CHIPS Inquiry Management: AskCHIPS - https://askchips.chips.gov
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
The reason why individuals can/cannot decline to provide PII/BII:
CHIPS Inquiry Management: Individuals may decline to provide PII/BII by not submitting an inquiry email or not completing the AskCHIPS webform. **CHIPS Portal: Applicants may decline registering in the Portal or providing information for a point of contact. In doing so, the Applicant will not be able to submit SOIs, Pre-Applications, or Applications.**

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

Yes
The reason why individuals can/cannot consent to particular uses of their PII/BII:
CHIPS Inquiry Management: Individuals are provided Privacy Act Statement at time of submission. Individuals provide consent to all uses included in the Notice. **CHIPS Portal: 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.

Yes
The reason why individuals can/cannot review/update PII/BII:
CHIPS Inquiry Management: Information provided 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. *(Check all that apply.)*

- **All NIST staff (employees and contractors) sign confidentiality agreement or non-disclosure agreements.**
- **All NIST staff are subject to a Code of Conduct that includes confidentiality protection requirements.**
- **Staff receive 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 High.**
- **NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 5 recommended security**

and privacy 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 and privacy assessment report has been reviewed for the supporting information system.** • **Contractors that have access to the system are subject to information security and privacy provisions in their contracts as required by DOC policy.** • **Contracts with customers establish ownership rights over data including PII/BII.** • **Access controls are in place as role-based permissions are used.**
Reason why access to the PII/BII is being monitored, tracked, or recorded:
To ensure access controls continue to operate as intended through annual continuous monitoring, logs, and through automated alerts and advisories from perimeter and application security defenses.
The information is secured in accordance with FISMA requirements.
This is a new system. An Assessment & Authorization (A&A) date will be provided when the A&A package is approved.
Other administrative and technological controls for the system:
N/A

8.2 Provide a 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 following statements apply to all NIST 201-01 CHIPS Program Management 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 181-04, Network Infrastructure System. 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 181-01, Network Security System.**

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, records in the system are covered by the following system of records notice (SORN).
SORN name, number, and link:
CHIPS Inquiry Management: DEPT-10, Executive Correspondence Files 79 FR 72623
SORN submission date to the Department:

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

Yes. Retention is monitored for compliance to the schedules listed.
Name of the record control schedule:
• **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**
The stage in which the project is in developing and submitting a records control schedule:
Reason why retention is not monitored for compliance to the schedule:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal
Records are disposed of via shredding and 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 of PII 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. *(Check all that apply.)*

Factors that were used to determine the above PII confidentiality impact levels	Explanation
The following apply to all PII maintained in the system:	**Identifiability: The data collected and maintained that can be used to identify specific individuals are limited (e.g., name and email) and deemed non-sensitive.** **Quantity of PII: The quantity of the PII that is collected and maintained pertains to members of the public.** **Context of Use: Customers provide information to obtain information about a product or service.** **Obligation to Protect Confidentiality: The organization is legally obligated to protect the PII.** **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. (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.)

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. **A risk exists with authorized users entering inaccurate information into CSfC modules.. This risk is mitigated through internal user training. A risk also exists with the general public entering incorrect information into the CHIPS Inquiry Management solution module. This risk is mitigated by allowing the general public to correct their information. In addition, the input field parameters have been limited in size to mitigate excessive input by the customer.**

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.
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

Points of Contact and Signatures

Information System Security Officer or System Owner	Chief Information Security Officer
Name: Li, Catherine Phone: Not available Email: catherine.li@chips.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: CATHERINE LI Digitally signed by CATHERINE LI Date: 2023.12.12 14:52:39 -05'00'	Name: Heiserman, Blair Phone: 301-975-3667 Email: nist-itso@nist.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: Digitally signed by BLAIR HEISERMAN Date: 2023.12.12 13:57:03 -05'00'
Co-Authorizing Official	**Authorizing Official**
Name: Wong, Jacob Phone: 240-205-6774 Email: jacob.wong@chips.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: JACOB WONG Digitally signed by JACOB WONG Date: 2023.12.13 06:56:29 -05'00'	Name: Sastry, Chandan Phone: 301-975-6500 Email: chandan.sastry@nist.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: CHANDAN SASTRY Digitally signed by CHANDAN SASTRY Date: 2023.12.12 14:34:17 -05'00'
Privacy Act Officer	**Chief Privacy Officer**
Name: Fletcher, Catherine Phone: 301-975-4054 Email: catherine.fletcher@nist.gov I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA. Signature: CATHERINE FLETCHER Digitally signed by CATHERINE FLETCHER Date: 2023.12.12 12:16:58 -05'00'	Name: Barrett, Claire Phone: 301-975-2852 Email: claire.barrett@nist.gov I certify that the PII/BII processed in this IT system is necessary and this PIA ensures compliance with DOC policy to protect privacy. Signature: CLAIRE BARRETT Digitally signed by CLAIRE BARRETT Date: 2023.12.11 15:44:08 -05'00'

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.