Template Version Number: 01-2021

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

Privacy Threshold Analysis
for the
201-01 CHIPS Program Office System

U.S. Department of Commerce Privacy Threshold Analysis

National Institute of Standards and Technology (NIST)

Unique Project Identifier: 201-01

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a brief description of the information system.*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

a) Whether it is a general support system, major application, or other type of system
b) System location
c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
d) The purpose that the system is designed to serve
e) The way the system operates to achieve the purpose
f) A general description of the type of information collected, maintained, use, or disseminated by the system
g) Identify individuals who have access to information on the system
h) How information in the system is retrieved by the user
i) How information is transmitted to and from the system

Provide a brief description of the information system.
The 201-01 CHIPS[1] Program Office (CPO) System supports DOC 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 components comprise the 201-01 CHIPS Program Office (CPO) System:

- **Parent: Provides Common Control inheritance to all subcomponents.**
- **Cloud-Salesforce CHIPS Org (CSfC): CSfC includes multiple subcomponents:**

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

  - **CHIPS Inquiry Management**
  - **CHIPS Incentives Portal**
- **Managed Windows Clients: Consists of end user desktops and laptops that are centrally managed.**
- **Networked Devices: Consists of end user resources (i.e., printers, copiers, and scanners).**

Of the components, the following stores, processes, or transmits PII and/or BII:

- **Cloud-Salesforce CHIPS Org (CSfC)**

The remainder of this PTA is scoped to the CSfC component.

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. The CHIPS Credit Subsidy Model subcomponent is utilized in Amazon Web Services under NIST 184-12, Infrastructure Services System, however no interconnection exists with other subcomponents.

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 purpose that the system is designed to serve

See introduction.

e. The way the system operates to achieve the purpose

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 Credit Subsidy Model*[2]**:** Used by NIST staff to generate accurate credit subsidy rate (CSR) estimates for loan applications to the CHIPS program in compliance with the Federal Credit Reform Act of 1990. The OMB Credit Subsidy Calculator (CSC) is integrated into the CHIPS Credit Subsidy Model in support of the estimates. The tool operates in the NIST Amazon Web Services (AWS) GovCloud environment with outputs inputted directly into the CSfC.
  - *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.

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

[2] Some documentation may refer to the Credit Subsidy Model as the CHIPS Obligation Model.

The CSfC component collects, maintains, uses, or disseminates the following types of information:

- **CHIPS Inquiry Management:** General Personal Data (GPD) and Work-Related Data (e.g., non-sensitive customer email and contact information)
- **CHIPS Incentives Portal:** Identifying Numbers (IN), General Personal Data (GPD), Work-Related Data (WRD), System Administration/Audit Data (SAAD), and Other PII or BII. WRD includes information about businesses submitting an application for CHIPS funding. WRD also includes 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).

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

The CSfC component has the following users:

- **CHIPS Inquiry Management:** authorized DOC and NIST employees and associates (to include contractors)
- **CHIPS Incentives Portal:** authorized DOC and NIST employees and associates (to include contractors), and third party reviewers. 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.

h. 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).

i. 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.

Questionnaire:

1. Status of the Information System

1a. What is the status of this information system?

This is a new information system in which changes create new privacy risks.
(Complete chart below, continue to answer questions, and complete certification.)

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:

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

Yes

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

NIST Special Publication 800-53 Rev. 5, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

No

Activities
Other activities which may raise privacy concerns:

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

Yes, the IT system collects, maintains, or disseminates BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

Yes, the IT system collects, maintains, or disseminates non-sensitive PII.

The IT system collects, maintains, or disseminates PII about:

General Public

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

No

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.
Provide the legal authority which permits the collection of SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

Yes

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

No

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the SAOP approved PIA must be a part of the IT system's Assessment and Authorization Package.

Is a PIA Required?	**Yes**

CERTIFICATION

__X__ The criteria implied by one or more of the questions above **apply** to the 201-01 CHIPS Program Office System and as a consequence of this applicability, a PIA will be performed and documented for this IT system.

____ The criteria implied by the questions above **do not apply** to the 201-01 CHIPS Program Office System and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Information System Security Officer or System Owner Name: Alderoty, Neil; Li, Catherine Phone: 301-975-8521; Not available Email: neil.alderoty@chips.gov; catherine.li@chips.gov Signature: NEIL ALDEROTY Digitally signed by NEIL ALDEROTY Date: 2023.11.17 15:45:15 -05'00' Date signed: _____ Signature: CATHERINE LI Digitally signed by CATHERINE LI Date: 2023.11.17 15:08:18 -05'00' Date signed: _____	**Chief Information Security Officer** Name: Heiserman, Blair Phone: 301-975-3667 Email: nist-itso@nist.gov Signature: Digitally signed by BLAIR HEISERMAN Date: 2023.11.20 10:42:48 -05'00' Date signed: _____
Co-Authorizing Official Name: Wong, Jacob Phone: 240-205-6774 Email: jacob.wong@chips.gov Signature: JACOB WONG Digitally signed by JACOB WONG Date: 2023.11.17 15:02:08 -05'00' Date signed: _____	**Authorizing Official** Name: Sastry, Chandan Phone: 301-975-6500 Email: chandan.sastry@nist.gov Signature: CHANDAN SASTRY Digitally signed by CHANDAN SASTRY Date: 2023.11.20 10:54:44 -05'00' Date signed: _____

Privacy Act Officer	**Chief Privacy Officer**
Name: Fletcher, Catherine Phone: 301-975-4054 Email: catherine.fletcher@nist.gov Signature: CATHERINE FLETCHER Digitally signed by CATHERINE FLETCHER Date: 2023.11.17 12:08:50 -05'00' Date signed: _____	Name: Barrett, Claire Phone: 301-975-2852 Email: claire.barrett@nist.gov Signature: CLAIRE BARRETT Digitally signed by CLAIRE BARRETT Date: 2023.11.17 08:02:30 -05'00' Date signed: _____