Version Number: 01-2019

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

Privacy Impact Assessment
for the
184-12 Infrastructure Services System

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

CATRINA PURVIS Digitally signed by CATRINA PURVIS
Date: 2020.08.12 09:49:21 -04'00' 08/12/2020

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: 184-12

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 Infrastructure Services System encompasses several enterprise infrastructure components (e.g., appliances) used to support the mission of NIST. This Privacy Impact Assessment (PIA) specifically addresses Content Collaboration, which is one component of this system. The purpose of Content Collaboration is to enable NIST to securely exchange sensitive information with the public.

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

The NIST Infrastructure Services System is a general support system.

b. System location

The component 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 NIST Infrastructure Services System is a standalone system.

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

The purpose of the Content Collaboration component is to enable NIST to securely exchange information with the public using either a secure file transfer mechanism or a collaborative workspace.

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

The initiating user must extend an invitation to another user to access and download information or utilize collaborative workspace.

f. How information is transmitted to and from the system

Information is transmitted to and from the system through user transactions. A typical transaction enables an authorized user to securely exchange information using either a secure file transfer mechanism or a collaborative workspace.

g. Any information sharing conducted by the system

The component does not share information with other internal NIST business units. However, information is shared through user transactions.

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..

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 01-2015)

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)
Other identifying numbers:
Explanation for the business need to collect, maintain, or disseminate the Social Security number, including

truncated form:

General Personal Data (GPD)
Email Address
Other general personal data:

Work-Related Data (WRD)
Work Email Address
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.

Directly from Individual about Whom the Information Pertains
Other
Other:
Authorized staff must invite an individual to use the component through an email generated by the staff using the component.

Government Sources
Other
Other:
Authorized staff must invite an individual from a government source to use the component through an email generated by the staff using the component.

Non-government Sources
Other
Other:
Authorized staff must invite an individual from a non-government source to use the component through an email generated by the staff using the component.

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

Accuracy of the information is the responsibility of the user.

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 **To promote information sharing initiatives**
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 Content Collaboration component requires invitation from an authorized staff member to individuals external to the organization. Individuals may represent themselves, Government, or non-Government sources.

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.)

Not applicable.

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.

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.

No, this IT system does not connect with or receive 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:

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

Class of Users
Other (specify)
Other:
Only invited individuals and the intended recipient(s) have access to the information exchanged.

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.

No, notice is not provided.
The Privacy Act statement and/or privacy policy can be found at:
The reason why notice is/is not provided:

Notice is not provided as the component requires invitation from an authorized staff member to individuals external to the organization.

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

Yes, individuals have an opportunity to decline to provide PII/BII.
The reason why individuals can/cannot decline to provide PII/BII:
Individuals have an opportunity to decline to provide PII/BII by not using the component.

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

Yes, individuals 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 have an opportunity to consent to particular uses of their PII/BII when collaborating with the staff member.

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

Yes, individuals have an opportunity to review/update PII/BII pertaining to them.
The reason why individuals can/cannot review/update PII/BII:
Individuals have opportunity to review/update PII/BII pertaining to them when authenticating to the component and reviewing their posting.

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system.

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 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).** **A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.**
Reason why access to the PII/BII is being monitored, tracked, or recorded:
Access logs for the component are kept and reviewed for anomalies on an as needed basis.

The information is secured in accordance with FISMA requirements.
Is this a new system? No **Below is the date of the most recent Assessment and Authorization (A&A).** **09/30/2019**
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 Component of the system is administered on internal NIST networks protected by multiple layers of firewalls. Access logs for the component are kept and reviewed for anomalies on an as needed basis. The component is located at the NIST Gaithersburg, Maryland facility within the continental United States. **Unauthorized use of the system is restricted by user authentication. Authorized staff must invite an individual to use the component through an email generated by the staff using the component. Invitation requires authentication by the invited individual through user authentication using a public web interface.** **For information sharing, information is stored in a secure fashion using FIPS 140-2 encryption. To guard against the interception of communication over the network, the component uses the Transport Layer Security (TLS) protocol which encrypts communications.**

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

No, the PII/BII is not 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."

No, this system is not a system of records and a SORN is not applicable.
SORN name, number, and link:
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?

No, there is not an approved record control schedule.
Name of the record control schedule:

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:
Authorized staff members using the component inherit responsibilities for information exchanged using the component.

10.2 Indicate the disposal method of the PII/BII.

Disposal
Other (specify)
Other disposal method of the PII/BII:
Information is deleted after 30 days of user account inactivity.

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**
Access to and Location of PII	**The component is located at the NIST Gaithersburg, Maryland facility within the continental United States. Staff authorized to use the component are the only individuals with access to the PII/BII.**

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.)

Threats to privacy could arise from misconfiguration of the Component by administrators. This threat is mitigated through routine assessment of security controls.

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