Version Number: 01-2019

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

Privacy Impact Assessment
for the
181-01 NIST Network Security

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: 2020.09.09 14:19:09 -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: 181-01

Introduction: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

(a) Whether it is a general support system, major application, or other type of system
(b) System location
(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
(d) The way the system operates to achieve the purpose(s) identified in Section 4
(e) How information in the system is retrieved by the user
(f) How information is transmitted to and from the system
(g) Any information sharing conducted by the system
(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information
(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

a) Whether it is a general support system, major application, or other type of system
The NIST Network Security System (181-01) (NNSS) provides network security components for all NIST information systems, which includes collection, management, and analyses of security information, event management data, logs, and other event data. The system has the following components:

- **Firewalls (FW),**
- **Intrusion Prevention/Detection Systems,**
- **SSL Remote Access (SSL RA),**
- **Security Implementation & Incident Response (SIIR),**
- **Asset Inventory and Network Access Control (NAC) (AI),**
- **System Support and/or Testing (SST),**
- **Network Monitoring and Vulnerability Scanning (NMVS), and**
- **Cyber Risk Scoring (CRS)**

b) System location
The components are located at the NIST Gaithersburg, Maryland and Boulder, Colorado facilities 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)

181-01 interconnects with other systems within the scope of its central purpose, for example: 181-04.

d) The way the system operates to achieve the purpose(s) identified in Section 4
The NNSS monitors and analyzes most all network traffic to identify actual or potential malicious attempts to alter the confidentiality, integrity, and availability of data. The FW and IDS components capture traffic flow (e.g., headers) and not the full packet. The full packet is captured in logs (e.g., all Internet traffic to and from NIST) and inspected by the SIIR component.
When traffic meets unacceptable criteria or an incident is reported, further investigation is conducted using system data and/or input from persons reporting. During an investigation or response to an incident, other data is pulled from network security logs (FW, IDS, full packet capture, servers, etc.) and stored/secured procedurally within the SIIR component. Information is copied to removable media and secured, thus preserving the chain of custody.
The Asset Inventory/Database (AI) is used to support Network Access Controls, and reconciles asset information obtained from other tools and user information (e.g., work-related data).

e) How information in the system is retrieved by the user
User retrieval is via authorized roles with limited permissions within network monitoring and inventory applications. General users do not have the ability to retrieve information containing PII from any system component. During an investigation, the incident response team are the only personnel authorized to retrieve data.

f) How information is transmitted to and from the system
Security Implementation & Incident Response Team (SIIRT) investigation data is sent to a team printer secured in the SIIRT office. All reports containing moderate impact data are hand-carried by SIIRT staff and given to authorized individuals. Users are required to report incidents via a secure .gov site. However, submission of the incident reports creates a plain text email notification to the affected individuals. When a NIST incident is declared, the incident is, in turn, reported to DoC in the format required by US-CERT.

g) Any information sharing conducted by the system

1. **Results from an investigation are shared with the supervisor or Human Resources (HR), Office of Inspector General, or Law Enforcement.**
2. **The system shares information as needed with DOC CIRT and US-CERT for cyber security awareness, and as needed within the bureau in support of incident handling.**

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 01-2017)

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)
File/Case ID
Other identifying numbers:
Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:

General Personal Data (GPD)
Name
Other general personal data:

Work-Related Data (WRD)
Work Address **Work Telephone Number** **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
Queries Run
ID Files Accessed
Contents of Files
Other system administration/audit data:

Other Information

2.2 Indicate sources of the PII/BII in the system.

Directly from Individual about Whom the Information Pertains
Other:

Government Sources
Within the Bureau
Other:

Non-government Sources
Other:

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

Information is protected from unauthorized access, modification, and deletion by encrypted access, policy, and user access controls which limits access to only authorized staff.

An integrity checker is used to enhance security of SIIRT (moderate impact) devices within this system. Components utilize a recommended integrity checker. Components also use system input restrictions such as character set, length, etc. to validate the entered data.

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?
Yes

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

Activities
Audio recordings
Electronic purchase transactions
Other
Other:
Video surveillance.

Section 4: Purpose of the System

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

Purpose
For administrative matters
Other:

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

Information is collected from NIST devices for cyber security purposes include: asset identification, log analysis, intrusion detection, vulnerability scanning, and incident handling.

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

Unauthorized access could result in a breach of users' information. Information system security controls used to protect this information are implemented, validated, and continuously monitored. NIST user access is restricted to authorized users. Annual training and rules of behavior are provided to internal users on the appropriate handling of PII. The components have records schedules and procedures in place to dispose of data accordingly.

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.

Case-by-Case – within the bureau **Case-by-Case - DOC bureaus** **Case-by-Case - Federal Agencies** **Other (specify) below**
Other:
Law Enforcement.

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

Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII.
The name of the IT system and description of the technical controls which prevent PII/BII leakage:
Because of the purpose of this system, traffic from all NIST information systems is captured by this system.

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

Class of Users
Government Employees **Contractors**
Other:

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system.

Yes, notice is provided 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.**
The Privacy Act statement and/or privacy policy can be found at:
The Privacy Act statement and/or privacy policy can be found at: https://www.nist.gov/privacy-policy.
The reason why notice is/is not provided:
Notice that PII is collected, maintained, or disseminated is provided by the login banner to the network.

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

No, individuals do not have an opportunity to decline to provide PII/BII.

The reason why individuals can/cannot decline to provide PII/BII:
Federal requirements subject users to monitoring. Users are required to agree to monitoring in general account rules of behavior before account credentials are issued.

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

No, individuals do not have an opportunity to consent to particular uses of their PII/BII.
The reason why individuals can/cannot consent to particular uses of their PII/BII:
Federal requirements subject users to monitoring. Users are required to agree to monitoring in general account rules of behavior before account credentials are issued.

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

No, individuals do not have an opportunity to review/update PII/BII pertaining to them.
The reason why individuals can/cannot review/update PII/BII:
Individual's data for information technology security incidents are not modified in case there is a need to provide for human resource or legal examination.

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system.

All users are subject to a Code of Conduct that includes the requirement for confidentiality. **Staff (employees and contractors) received training on privacy and confidentiality policies and practices.** **Access to the PII/BII is restricted to authorized personnel only.** **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).**
Reason why access to the PII/BII is being monitored, tracked, or recorded:
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).** **04/1/2020**
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 system components are administered on internal NIST networks. The components are at various locations within the continental United States. **Use of the components is restricted by user authentication, and role-based access is employed across all components.** **To guard against the interception of communication over the network, the component uses the Transport layer Security (TLS) protocol which encrypts communications. PII/BII is transferred in a secure fashion using FIPS 140-2 encryption when sharing incident information.**

Section 9: Privacy Act

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

Yes, the PII/BII is searchable by a personal identifier.

9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

Yes, this system is covered by an existing system of records notice (SORN).
SORN name, number, and link:
Commerce/DEPT-25, Access Control and Identity Management System
SORN submission date to the Department:

Section 10: Retention of Information

10.1 Are these records are covered by an approved records control schedule and monitored for compliance?

Yes, there is an approved record control schedule.
Name of the record control schedule:
General Records Schedule 3.2
The stage in which the project is in developing and submitting a records control schedule:
Yes, retention is monitored for compliance to the schedule.
Reason why retention is not monitored for compliance to the schedule:

10.2 Indicate the disposal method of the PII/BII.

Disposal
Shredding
Degaussing
Deleting
Other disposal method of the PII/BII:

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

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

11.2 The factors that were used to determine the above PII confidentiality impact levels.

Factors that were used to determine the above PII confidentiality impact levels	Explanation
Quantity of PII **Obligation to Protect Confidentiality** **Access to and Location of PII**	**Quantity of PII-Collectively, the number of records maintained generate a large amount of PII and a breach in such large numbers of individual PII is considered in the determination of the impact level. The volume of data transmitted within logs that may include other personally identifiable information is unknown.** **Obligation to Protect Confidentiality-Based on the type of data which could be within the system, it must protect (e.g., via encryption) the BII/PII of each individual in accordance with the Privacy Act of 1974.** **Access to and Location of PII-Use of the components is restricted by user authentication, and role-based access is employed across all components (i.e., only privileged user access). Physical security controls are restricted on each component.**

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. **The NNSS functionality replaces several different existing on-premise systems, but includes no new use of information from already approved solutions. This reduces the need to implement additional solutions for new requirements.** **The use of NNSS service eliminates NIST's need to store and process users' information locally, reducing risk associated with sensitive data.**

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