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

Privacy Threshold Analysis
for the
181-01 NIST Network Security

U.S. Department of Commerce Privacy Threshold Analysis

National Institute of Standards and Technology (NIST)

Unique Project Identifier: 181-01

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 general description (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

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

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),**
- **Cyber Risk Scoring (CRS), and**
- **Management of Rules of Behavior (ROB)**

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 purpose that the system is designed to serve
The NIST Network Security System (181-01) (NNSS) provides network security components for all NIST information systes, which includes collection, management, and analyses of security information, event management data, logs, and other event data.

e) The way the system operates to achieve the purpose
The NIST Network Security System 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. 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).

f) A general description of the type of information collected, maintained, use, or disseminated by the system
The type of information includes the basics required for incident monitoring/reporting, including: file/case ID, name, work-related data and system administration/audit data.

g) Identify individuals who have access to information on the system
Only authorized individuals have role-based access to include the SIIRT team.

h) 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.

i) How information is transmitted to and from the system
Security Intelligence & Incident Response Team (SIIRT) investigation data is sent to a team printer secured in the SIIRT Team Lead's 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 required formatted email, mandated by US-CERT.

Questionnaire:

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 or later).
   (Skip questions and complete certification)

Changes That Create New Privacy Risks (CTCNPR)
Other changes that create new privacy risks:

2. Is the IT system or its information used to support any activity which may raise privacy concerns?
   NIST Special Publication 800-53 Revision 4, Appendix J, 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.

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.)."

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."

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

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?

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?

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.

Is a PIA Required?	**Yes**

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 approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X__ I certify the criteria implied by one or more of the questions above **apply** to the 181-01 NIST Network Security and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the 181-01 NIST Network Security and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO):

Heiserman, Blair

Signature of SO: Digitally signed by BLAIR HEISERMAN Date: 2020.12.23 12:00:08 -05'00' Date: ___________

Name of Co-Authorizing Official (Co-AO):

Signature of Co-AO: _______________N/A______________________ Date: ___________

Name of Information Technology Security Officer (ITSO):

Tweedy, Romain

Signature of ITSO: AARON TWEEDY Digitally signed by AARON TWEEDY Date: 2020.12.22 10:24:47 -05'00' Date: ___________

Name of Authorizing Official (AO):

Sastry, Chandan

Signature of AO: CHANDAN SASTRY Digitally signed by CHANDAN SASTRY Date: 2020.12.22 11:21:29 -05'00' Date: ___________

Name of Privacy Act Officer (PAO):

Fletcher, Catherine

Signature of PAO: CATHERINE FLETCHER Digitally signed by CATHERINE FLETCHER Date: 2020.12.23 10:35:36 -05'00' Date: ___________

Name of Bureau Chief Privacy Officer (BCPO):

Schiller, Susannah

Signature of BCPO: SUSANNAH SCHILLER Digitally signed by SUSANNAH SCHILLER Date: 2020.12.23 10:25:35 -05'00' Date: ___________