Version Number: 01-2019

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

Privacy Threshold Analysis
for the
610-02 NIST Center for Neutron Research

U.S. Department of Commerce Privacy Threshold Analysis

National Institute of Standards and Technology (NIST)

Unique Project Identifier: 610-02

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

The NIST Center for Neutron Research (NCNR) is a National User Facility for neutron scattering research. Its primary function is scientific research and development of methods for measuring physical and chemical properties of matter, in collaboration with external users. The NCNR Laboratory Computing System supports administration and management of facility and equipment access.

a. Whether it is a general support system, major application, or other type of system
The NIST Center for Neutron Research (NCNR) Laboratory Computing System is a general support system.

b. System location

The NCNR Laboratory Computing System components are 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 NCNR Laboratory Computing System is a standalone system.

d. The purpose that the system is designed to serve
NCNR's primary function is scientific research and development of methods for measuring physical and chemical properties of matter, in collaboration with external users.

e. The way the system operates to achieve the purpose
The NCNR Laboratory Computing System supports administration and management of facility and equipment access through the following components:

The Information Management System (IMS) supports soliciting and reviewing proposals for scientific experiments at NCNR and allocating instrument time through a web portal. The portal also includes submission of information to process individuals in systems to ensure work agreements are in place, and to ensure scheduled facility users have access to the campus.

The NCNR physical access system enables multi-level access controls within the facility, limiting access to the Reactor Operator area. Motion detection recording cameras are in controlled areas (e.g., chemistry labs) to support detection of unauthorized access and either single or combined biometrics are also used. All biometrics are on the Reactor Security Network (RSN) that is required by an agency external to NIST. RSN is a vendor-maintained badge-access system that is deployed to provide more restrictive access to the nuclear laboratories. However, RSN does not connect to the NIST network and is confined to just the NCNR building.

f. A general description of the type of information collected, maintained, use, or disseminated by the system
The type of information includes: identifying numbers, general personal data, work-related data, distinguishing features/biometrics, and system administration/audit data.

g. Identify individuals who have access to information on the system
The NCNR Laboratory Computing System is accessed by authorized NIST staff. The interface allows information to be retrieved by the person who registered and created an individual profile.

h. How information in the system is retrieved by the user
The NCNR Laboratory Computing System allows information to be retrieved by the person who registered and created an individual profile. Public users can only retrieve their own profile information. Authorized NIST users retrieve information directly from the component.

i. How information is transmitted to and from the system
The NCNR Laboratory Computing System obtains information by (1) identifying people who have been invited to register for NCNR facilities use; and (2) managing non-sensitive customer email and contact information.

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.

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.

Is a PIA Required?	**Yes**

CERTIFICATION

__X__ I certify the criteria implied by one or more of the questions above **apply** to the 610-02 NIST Center for Neutron Research - Lab and Admin Systems 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 610-02 NIST Center for Neutron Research - Lab and Admin Systems and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO):

Munter, Alan

Signature of SO: Alan E Munter Digitally signed by ALAN MUNTER Date: 2021.02.17 10:03:25 -05'00' Date: ____________

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

Dimeo, Robert

Signature of Co-AO: ROBERT DIMEO Digitally signed by ROBERT DIMEO Date: 2021.02.24 12:02:43 -05'00' Date: ____________

Name of Information Technology Security Officer (ITSO):

Heiserman, Blair

Signature of ITSO: Digitally signed by BLAIR HEISERMAN Date: 2021.01.25 13:42:33 -05'00' Date: ____________

Name of Authorizing Official (AO):

Sastry, Chandan

Signature of AO: CHANDAN SASTRY Digitally signed by CHANDAN SASTRY Date: 2021.02.19 16:48:04 -05'00' Date: ____________

Name of Privacy Act Officer (PAO):

Fletcher, Catherine

Signature of PAO: CATHERINE FLETCHER Digitally signed by CATHERINE FLETCHER Date: 2021.01.19 09:00:29 -05'00' Date: ____________

Name of Acting Bureau Chief Privacy Officer (BCPO):

Wilkinson, Matt

Signature of Acting BCPO: MATTHEW WILKINSON Digitally signed by MATTHEW WILKINSON Date: 2021.01.26 09:16:17 -05'00' Date: ____________