Version Number: 01-2019

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

Privacy Impact Assessment
for the
610-02 NIST Center for Neutron Research - Lab and Admin Systems

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

Jennifer Goode for Dr. Catrina D. Purvis 10/02/2020

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: 610-02

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. A general description of the information in 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.

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

e. 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.

f. 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.

g. Any information sharing conducted by the system
The components will share information with other internal NIST business units, and other Federal entities as required by law. Occasional summary reports on foreign researcher participation, diversity/minority statistics, and instrument/sample data is shared internally and provided to other federal agencies such as NSF. However, these summaries do not contain personal identifiers.

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.

27 Stat. 395 and 31 Stat. 1039, and all existing, applicable NIST and Department policies, regulations and directives concerning the tracking, security processing, and support of NAs during their tenure at NIST.

Section 107, 161(i), Atomic Energy Act of 1954 as amended; 42 U.S.C. 2137, and 202l(i); 15 U.S.C. 272.

5 U.S.C. 301; 35 U.S.C. 2; the Electronic Signatures in Global and National Commerce Act, Public Law 106-229; 28 U.S.C. 533-535; 44 U.S.C. 1301; Homeland Security Presidential Directive 12 and IRS Publication-1075.

i. The Federal Information Processing Standard (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 or later)

Changes That Create New Privacy Risks (CTCNPR)
N/A
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)
Social Security **Driver's License** **Passport**
Other identifying numbers:
Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:
National Identity Number. **SSN and National Identity Number are required to process transactions necessary for preparation of the agreement and for access to the facility.**

General Personal Data (GPD)
Name **Gender** **Race/Ethnicity** **Date of Birth** **Place of Birth** **Home Address** **Telephone Number** **Email Address** **Other general personal data**
Other general personal data:
Citizenship **Permanent Residence/Green Card Holder**

Work-Related Data (WRD)
Occupation
Job Title
Work Address
Work Telephone Number
Work Email Address
Other work-related data
Other work-related data:
Affiliation

Distinguishing Features/Biometrics (DFB)
Fingerprints
Retina/Iris Scans
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
In Person
Online
Other:

Government Sources
Within the Bureau
Other Federal Agencies
Other:

Non-government Sources
Other:

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

Integrity controls have been assessed per those controls defined in NIST Special Publication 800-53. Verification of information occurs against hardcopy documentation upon arrival (e.g., driver's license, passport).

2.4 Is the information covered by the Paperwork Reduction Act?

Yes, the information is covered by the Paperwork Reduction Act.
The OMB control number and the agency number for the collection:
OMB Control #0693-0081

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)
N/A
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
Building entry readers **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).

NCNR collects data about the NCNR facility users in order to carry out its programmatic goal of administering the National User Facility scientific program. This program consists of soliciting and reviewing proposals for scientific experiments at NCNR, allocating instrument time, managing the resulting site visits and resulting scientific data and publications. Information collected within the components include federal employees/contractors, and Associates (foreign or domestic).

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 as the research results are intended for publication. **There exists a privacy threat to General Personal Data (GPD) until the information is entered into the NIST Associate Information System. Role-based access is employed as only those who are authorized to perform the data entry have access to the GPD. This staff is trained in handling this type of information.**

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 - DOC bureaus **Case-by-Case - Federal Agencies** **Case-by-Case - 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
General Public
Government Employees
Contractors
Other (specify)

Other:
General Public class of users is limited to those with a submitted and approved proposal. **Contractors class of users includes NIST Associates (foreign or domestic).**

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.**
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 Privacy Act Statement is found when a user registers and accesses the IMS, which is initiated from https://www-s.nist.gov/NCNR-IMS/login.do.**
The reason why notice is/is not provided:

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:
PII/BII must be provided for review of proposals and for facility access. Individuals choose whether to utilize the NCNR if accepted. Individuals may choose to decline to provide PII/BII and not utilize the NCNR.

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 opportunity to consent to particular uses of their particular uses of their information upon registering a profile within IMS. The registration profile provides the requisite Privacy Act Statement.

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 may register and log in to the IMS and review/update information pertaining to them.

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.** **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.** **Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.**
Reason why access to the PII/BII is being monitored, tracked, or recorded:
Access is restricted to only employees and contractors with a "need to know" and is tracked and recorded through system logs.
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).** **04/01/2020**
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 components of the system are accessible on internal NIST networks protected by multiple firewalls. Unauthorized use of the system is restricted by user authentication. Access to logs are kept and reviewed for anomalies on an as needed basis. Data is stored on servers located at the NIST Gaithersburg, Maryland, facility within the continental United States. **The data is encrypted at rest. Physical access controls are employed on a separate, isolated network.** **General Personal Data (GPD) is deleted following data entry into the NIST Associate Information System.**

Section 9: Privacy Act

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

Yes, 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:
NIST-1, NIST Associates (section for Facility User Records for NCNR) **NIST-5, Nuclear Reactor Operator Licensees File** **DEPT-6, Visitor Logs and Permits for Facilities Under Department Control** **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:
GRS 5.6, Security Records **NIST Records Schedule 104-107, Nuclear Reactor Program Records** **General Personal Data (GDP) is deleted following data entry into the NIST Associate Information System**
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 **Overwriting** **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
Identifiability **Context of Use** **Obligation to Protect Confidentiality** **Access to and Location of PII**	**Identifiability- Processing of proposers for facility access requires submission of General Personal Data.** **Context of Use- Proposed data research results are intended for publication.** **Obligation to Protect Confidentiality- NCNR reputation would be affected if is failed to protect non-public data.** **Access to and Location of PII- General Personal Data is immediately deleted after data entry into the NIST Associate Information System occurs.**

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.)

Not applicable as the research results are intended for publication.

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