Version Number: 01-2019

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

Privacy Impact Assessment
for the
680-01 Physical Measurement Laboratory General Support System

Reviewed by: Matt Wilkinson, Acting 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 09/17/2021

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: 680-01

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

The NIST Physical Measurement Laboratory (PML) operates a National, shared-use facility for nanoscale fabrication and measurement, and develops innovative nanoscale measurement and fabrication capabilities to support researchers from industry, academia, NIST, and other government agencies in nanoscale technology from discovery to production. The PML System supports administration and management of the NanoFab facility and equipment access through the following:

- **Application to use the facility requires submission of a Project. The forms are available for public download, and are required to be mailed, faxed, or emailed. Internal users also have the option to submit the form through the internal NIST homepage.**
- **The NanoFab Billing System (NBS) provides centralized accounting, fund and tool usage fee management for the NanoFab facility.**
- **The NanoFab physical access control system enables access controls on the internal access points within the building, limiting access to the NanoFab. In addition, a camera monitoring system enables remote monitoring of the NanoFab to support detection of unauthorized access.**

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

b. System location

The system 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 Physical Measurement Laboratory (PML) System is a standalone system.

d. The way the system operates to achieve the purpose(s) identified in Section 4
Following submission of a project application, if accepted, time is scheduled for use of the NanoFab facility, and payment made to NIST for hours utilized.

e. How information in the system is retrieved by the user
Users are able to request information by contacting the NanoFab User Office or NanoFab Manager.

f. How information is transmitted to and from the system
Information is transmitted over the NIST internal network.

g. Any information sharing conducted by the system
The components will share information with other internal NIST business units.

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.

5 U.S.C. App.—Inspector General Act of 1978, § 2; 5 U.S.C. App.—Reorganization Plan of 1970, § 2; 13 U.S.C. § 2; 13 U.S.C. § 131; 15 U.S.C. § 272; 15 U.S.C. § 1151; 15 U.S.C. § 1501; 15 U.S.C. § 1512; 15 U.S.C. § 1516; 15 U.S.C. § 3704b; 16 U.S.C. § 1431; 35 U.S.C. § 2; 42 U.S.C. § 3121 et seq.; 47 U.S.C. § 902; 50 U.S.C. App. § 2401 et seq.; E.O. 11625; 77 FR 49699 (Aug. 16, 1012).

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 or later).

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)
Name
Other general personal data:

Work-Related Data (WRD)
Work Address **Work Telephone Number** **Work Email Address** **Business Associates** **Other work-related data**
Other work-related data:
Business proprietary information.

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
Hard Copy - Mail/Fax **Online** **Email** **Other**
Other:
Public downloadable PDF.

Government Sources

Other:

Non-government Sources
Other:

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

The integrity of information is ensured by the individual submitting information (e.g., on forms).

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 #0693-0067

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
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).

Following submission of a project application, time is scheduled for use of the NanoFab facility, and payment made to NIST for hours utilized. Information is collected for federal/employee/contractors, Associates (foreign or domestic), or members of the public.

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.)

Potential threats to privacy include the insider threat (e.g., authorized users misusing data or authorized user inadvertently combining multiple data sets resulting in aggregation of personal data). **Mitigating controls include employing and monitoring administrative access, training for administrators, and assurance of compliance to records management schedules.**

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
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 project. **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 by other means.
The Privacy Act statement and/or privacy policy can be found at:
The reason why notice is/is not provided:
Notice is provided on the forms required for submission.

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 opportunity to decline to provide PII/BII and not submit the requisite documentation. However, doing so would prohibit use of the facility, instrumentation, and related resources.

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 PII/BII when submitting documentation.

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 submitting documentation.

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system.

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.**

Reason why access to the PII/BII is being monitored, tracked, or recorded:
Access is restricted only for 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).** **04/01/2021**
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 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. **Financial data is transmitted securely on internal networks.**

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:
NIST-1: NIST Associates
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 1.1 Financial Management and Reporting **GRS 3.1 General Technology Management Records** **GRS 5.6 Security Records**
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.)*

Low – the loss of confidentiality, integrity, or availability could be expected to have a limited 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
Context of Use **Obligation to Protect Confidentiality**	**Context of Use-Project data research results are intended for publication.** **Obligation to Protect Confidentiality-PML reputation would be affected if it failed to project non-public data.**

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.)

Potential threats to privacy include the insider threat (e.g., authorized users misusing data or authorized user inadvertently combining multiple data sets resulting in aggregation of personal data). **Mitigating controls include employing and monitoring administrative access, training for administrators, and assurance of compliance to records management schedules.**

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