U.S. Department of Commerce
National Institute of Standards and Technology

Privacy Threshold Analysis
for the
Physical Measurement Laboratory Support System (PML)
(680-01)
U.S. Department of Commerce Privacy Threshold Analysis
National Institute of Standards and Technology/
Center for Nanoscale Science and Technology

Unique Project Identifier: 680-01

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 of the information system in a way that a non-technical person can understand.
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).

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 Physical Measurement Laboratory (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.
- The NanoFab Billing System (NBS) provides centralized accounting, fund and tool usage fee management for the NanoFab facility.
- The PML 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
   The Physical Measurement Laboratory (PML) System is a general support system.

b) System location
   The Physical Measurement Laboratory (PML) 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 purpose that the system is designed to serve
The PML System operates a National, shared-use facility for nanoscale fabrication and measurement, and develops innovative nanoscale measurement and fabrication capabilities.

e) The way the system operates to achieve the purpose
Following submission of a project application, time is scheduled for use of the NanoFab facility, and payment made to NIST for hours utilized.

f) A general description of the type of information collected, maintained, use, or disseminated by the system
General personal data (GPD) and work-related data (WRD) necessary to support the administration and management of the NanoFab facility and equipment access. Project applications may contain business proprietary information.

g) Identify individuals who have access to information on the system
Authorized NIST staff have access to the PML System.

h) How information in the system is retrieved by the user
Users are able to request information about their project application by contacting the NanoFab User Office or NanoFab Manager.

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

Questionnaire:

1. What is the status of this information system?

___ This is a new information system. Continue to answer questions and complete certification.

_X__ This is an existing information system with changes that create new privacy risks.

Complete chart below, continue to answer questions, and complete certification.

<table>
<thead>
<tr>
<th>Changes That Create New Privacy Risks (CTCNPR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Conversions</td>
</tr>
<tr>
<td>b. Anonymous to Non-Anonymous</td>
</tr>
<tr>
<td>c. Significant System Management Changes</td>
</tr>
<tr>
<td>j. Other changes that create new privacy risks (specify):</td>
</tr>
</tbody>
</table>

___ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. Continue to answer questions and complete certification.
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 01-2015 or later). Skip questions and complete certification.

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.

_X_ Yes. Please describe the activities which may raise privacy concerns.
Facility camera monitoring

_X_ Yes, the IT system collects, maintains, or disseminates BII about: (Check all that apply.)

_X_ Companies

____ Other business entities

____ No, this IT system does not collect any BII.

4. Personally Identifiable Information
4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?
As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

_X_ Yes, the IT system collects, maintains, or disseminates PII about: (Check all that apply.)

_X_ DOC employees

_X_ Contractors working on behalf of DOC

_X_ Members of the public
No, this IT system does not collect any PII.

If the answer is “yes” to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

___ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

___ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. 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.

___ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

___ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c 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 Physical Measurement Laboratory (PML) System (680-01) 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 Physical Measurement Laboratory (PML) (680-01) and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO):
James G. Kushmerick. Acting
Signature of ISSO or SO: ____________________________ Date: 9/27/2019

Name of Information Technology Security Officer (ITSO):
K. Robert Glenn
Signature of ITSO: KENNETH GLENN Digitally signed by KENNETH GLENN
Date: 2019.09.27 09:00:43 -04'00'

Name of Co-Authorizing Official (AO):
Carl Williams. Acting
Signature of AO: ____________________________ Date: 9/27/2019

Name of Co-Authorizing Official / Bureau Chief Privacy Officer (BCPO):
Susannah Schiller. Acting
Signature of AO/BCPO: SUSANNAH SCHILLER Digitally signed by SUSANNAH SCHILLER
Date: 2019.09.27 10:23:00 -04'00'