Version Number: 01-2019

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

Privacy Threshold Analysis
for the
100-02 Associate Directors' Staff Offices System

U.S. Department of Commerce Privacy Threshold Analysis

National Institute of Standards and Technology (NIST)

Unique Project Identifier: 100-02

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

a. Whether it is a general support system, major application, or other type of system
The Associate Director's Offices System (100-02) is a general support system.

b. System location
The components are located at the NIST Gaithersburg, Maryland facility and in Culpepper, Virginia.

c. Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
The Associate Director's Offices System (100-02) is a standalone system.

d. The purpose that the system is designed to serve

NIST administers the National Voluntary Laboratory Accreditation Program (NVLAP). NVLAP provides accreditation services through various laboratory accreditation programs (LAPs), which are established on the basis of requests and demonstrated need. Each LAP includes specific test or calibration standards and related methods and protocols assembled to satisfy the unique needs for accreditation in a field of testing or calibration. NVLAP accredits public and private laboratories based on evaluation of their technical qualifications and competence to carry out specific calibrations or tests. The rNIS application assists in administering activities associated with this mission.

NIST builds and sustains technology partnering activities between the NIST laboratories and industries in the U.S., local, state and federal agencies, and the general public. The Tech Transfer application assists in administering activities associated with this mission. The Reimbursable Agreements Coordination Office (RACO) was established to standardize NIST-wide policies and procedures related to the preparation, processing, coordination, execution, of Payable and Reimbursable Agreements. The RACO Agreements Application assists in administering activities associated with this mission.

e. The way the system operates to achieve the purpose

- **rNIS: The rNIS component helps manage the NIST National Voluntary Laboratory Accreditation Program (NVLAP) accreditation process to capture, process, and analyze data provided by laboratories applying for accreditation. The internal NVLAP program staff use rNIS to store and process the data for accreditation applications. The application enables:**
  a) **Submission of application documents online, and obtaining results of the accreditation after the process is complete.**
  b) **Management application workflow and generate the reports used by NVLAP personnel in support of the NVLAP accreditation program.**
  c) **Tracking of accreditation history for each laboratory.**
  d) **Generation of laboratory letters in support of the accreditation process (i.e., reminder and expiration letters).**
- **Tech Transfer: The Tech Transfer application manages, tracks, and reports on the creation, review, and approval processes for Cooperative Research and Development Agreements Licenses, Materials Transfer Agreements (MTA), Data Transfer Agreements (DTA), and Non-Disclosure Agreements (NDA), facilitate disclosure of inventions, and facilitate, track, and report on the status of patent Applications. This application streamlines approval and disclosure process, and provides transparency to customers, leadership, and various groups involved in the processes.**
- **Reimbursable Agreements Coordination Office (RACO) Agreements Application: The RACO Agreements Application enables review of reimbursable and payable agreements between NIST and external partners.**

f. A general description of the type of information collected, maintained, use, or disseminated by the system

rNIS: The General Personal Data and Work-Related Data collected, analyzed, and processed includes laboratory on-site assessment results as well as basic contact information for the Points of Contact at the laboratories.

Tech Transfer: The General Personal Data and Work-Related Data collected, analyzed, and processed includes information related to invention disclosures, patents, and collaborations that support NIST research-related projects and activities. All sensitive information is stored in the Attachment Application (183-01).

RACO Agreements Application: The General Personal Data and Work-Related Data collected, analyzed, and processed includes reimbursable and payable agreements between NIST and its partners. This includes Federal interagency agreements and non-Federal agreements with other organizations in which NIST will receive or provide research, goods, or services.

g. Identify individuals who have access to information on the system
Participating organizations may access the rNIS application to submit application and accreditation results.
Only authorized NIST staff have access to the Tech Transfer and RACO Agreements Application.

h. How information in the system is retrieved by the user
The information is retrieved by the user by first logging in via the authentication/login capabilities and then accessing the information needed to conduct NIST work.

i. How information is transmitted to and from the system
Information is submitted directly in, and is stored within, these components.

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 100-02 Associate Directors' Staff Offices System 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 100-02 Associate Directors' Staff Offices System and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO):

Herman, Michael

Signature of SO: MICHAEL HERMAN Digitally signed by MICHAEL HERMAN Date: 2021.01.04 09:36:44 -05'00' Date: _____

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

Kimball, Kevin

Signature of Co-AO: KEVIN KIMBALL Digitally signed by KEVIN KIMBALL Date: 2021.01.07 17:24:34 -05'00' Date: _____

Name of Information Technology Security Officer (ITSO):

Heiserman, Blair

Signature of ITSO: Digitally signed by BLAIR HEISERMAN Date: 2020.12.23 12:04:51 -05'00' Date: _____

Name of Authorizing Official (AO):

Sastry, Chandan

Signature of AO: CHANDAN SASTRY Digitally signed by CHANDAN SASTRY Date: 2020.12.22 11:16:53 -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 10:40:38 -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 11:16:05 -05'00' Date: _____