Version Number: 01-2019

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

Privacy Impact Assessment
for the
100-02 Associate Directors' Staff Offices System

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

CATRINA PURVIS Digitally signed by CATRINA PURVIS
Date: 2020.12.08 07:30:13 -05'00'

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer

10/02/2020
Date

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

Unique Project Identifier: 100-02

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. 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 way the system operates to achieve the purpose(s) identified in Section 4

- **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:**
- **Submission of application documents online, and obtaining results of the accreditation after the process is complete.**
- **Management application workflow and generate the reports used by NVLAP personnel in support of the NVLAP accreditation program.**

- **Tracking of accreditation history for each laboratory.**
- **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.**

e. How information in the system is retrieved by the user

- **rNIS: Authorized NIST users may retrieve information based on their role and share output on a case by case basis for purposes of oversight and management. Authorized representatives of participating organizations may retrieve information about their own accreditation process and outcome. Information is retrieved based on an organizational identifier.**
- **Tech Transfer: Authorized NIST users may retrieve information based on their role. Output may be shared on a case by case basis for purposes of oversight and management. Inventors, some of whom are foreign citizens, are authorized NIST users who may retrieve information about their own inventions.**
- **RACO Agreements Application: Authorized NIST users may retrieve information based on their role and share output on a case by case basis for purposes of oversight and management.**

f. How information is transmitted to and from the system

Participating organizations may access the rNIS application to submit application and accreditation results.

Information is submitted directly into the applications by NIST staff. Sensitive information is stored (for Tech Transfer and RACO Agreements) in an Attachment Application.

g. Any information sharing conducted by the system

Authorized NIST users may retrieve information based on their role and share output on a case by case basis for purposes of oversight and management.

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, 1 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.

Accreditation requiements are established in accordance with the U.S. Code of Federal Regulations (CFR, Title 15, Parts 272 and 285), National Voluntary Laboratory Accreditation Program, and encompass the requirements of ISO/IEC 17025.

Programmatic authorities include 15 U.S.C. 3710a, Cooperative Research and Development Agreements; 35 U.S.C. 207, Domestic and Foreign Protection of Federally Owned Inventions; 37 U.S.C., Patents, Trademarks, and Copyrights; 15 U.S.C. 202-209 (Bayhle-Dole Act); 15 U.S.C. 3710(g) (Federal Transfer Act); Executive Order 12591, Facilitating Access to Science and Technology.

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
Maiden Name
Telephone Number
Email Address
Other general personal data
Other general personal data:
Citizenship

Work-Related Data (WRD)
Job Title
Work Address
Work Telephone Number
Work Email Address
Other work-related data
Other work-related data:
Employer
Fax number

Distinguishing Features/Biometrics (DFB)
Other distinguishing features/biometrics:

[illegible] Data (SAAD)
User ID
IP Address
Date/Time of Access
Other system administration/audit data:

Other Information
Intellectual property related data (e.g., patent named inventor) and any associated patent-related business endeavors. **NIST inventions, patents, disclosures, agreements, and results of assessments performed by accreditation laboratories.**

2.2 Indicate sources of the PII/BII in the system.

Directly from Individual about Whom the Information Pertains
In Person
Telephone
Hard Copy - Mail/Fax
Email
Online
Other:

Government Sources
Within the Bureau
Other Federal Agencies
Other:

Non-government Sources
Public Organizations
Private Sector
Other:

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

If any of the information needs clarification, authorized/designated NIST staff contact the individual that provided the information to ensure accuracy of the information.

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 Numbers 0693-0033, 0693-0031, 063-0003, and 0693-0085

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?

No

The IT system supported activities which raise privacy risks/concerns.

Activities
Other:

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 **To improve Federal services online**
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).

rNIS: Information collected is regarding public organizations (e.g., the laboratory seeking accreditation services) during both the application process and accreditation assessments.

Tech Transfer: Information collected is in reference to federal employees for administration of potential patents or collaborations. **RACO Agreements: Information collected is in reference to members of the public who seek to enter into agreement with NIST.**

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 data). Information collected is limited to only that which is needed for the service. **Mitigating controls include employing and monitoring administrative access, periodic review of roles, training for administrators and users, issuance of rules of behavior for roles, 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 - DOC bureaus
Case-by-Case - Federal Agencies
Case-by-Case - Within the bureau
Direct Access - Foreign entities
Direct Access - Private sector
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.

Yes, this IT system connects with or receives 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:
NIST 188-01, Platform Services Division System (infrastructure)

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:

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.

Yes, notice is provided by other means.

The Privacy Act statement and/or privacy policy can be found at:

The Privacy Policy can be found at: https://www.nist.gov/privacy-policy. Privacy Act Statements are accessible for Tech Transfer and RACO Agreements on the internal application interfaces.

The reason why notice is/is not provided:

rNIS: Work-related data of the Authorized Representative (AR) from each accredited laboratory is provided as part of the accreditation application process, which identifies the uses of this information.

RACO Agreements: Users are offered notice via the forms provided as part of the Application process.

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:

rNIS: Opportunity to decline work-related data is made available through the application process. A laboratory will be denied an accreditation by refusing to identify an Authorized Representative (AR).

Tech Transfer: Opportunity to decline providing information is made available through the application process.

RACO Agreements: Opportunity to decline providing information is made available through the application process.

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:

rNIS: Opportunity to consent to particular uses of work-related data is made available through the application process and described in the NIST Handbook 150. A laboratory will be denied an accreditation by refusing to consent to particular uses as described.

Tech Transfer: Consent is implied as participants are requesting to begin either an invention disclosure or collaboration/agreement process.

RACO Agreements: Consent is implied as participants are requesting to enter into an agreement with NIST.

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:
rNIS: Authorized Representatives may review/update work-related data directly in the application. **Tech Transfer: PII/BII is provided by the user and therefore should be accurate at the time it is provided.** **RACO Agreements: Information provided may be updated prior to agreement finalization through their NIST contract.**

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.

Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.

Other (specify)

Reason why access to the PII/BII is being monitored, tracked, or recorded:
Access logs are kept and reviewed for anomalies on an as-needed basis.

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:
Both Tech Transfer and RACO Agreements use the Attachment Application, which enables encryption of data at rest.

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 are accessible on internal NIST networks protected by multiple layers of firewalls. Unauthorized use of the system is restricted by user authentication (for both NIST users and Authorized Representatives from accredited laboratories). Access logs are kept and reviewed for anomalies on an as-needed basis.

To guard against the interception of communication over the network, rNIS uses the Transport Layer Security (TLS) protocol which encrypts communications for the external (internet-facing) component for the accredited laboratory's use. **The Tech Transfer and RACO Agreements components use the Attachment Application for storing sensitive information (e.g., encrypted). The Attachment Application is hosted, maintained, and administered by, and located at NIST. Otherwise, data is stored on servers located at the NIST Gaithersburg, Maryland facility (rNIS), and Culpepper, Virginia (Tech Transfer and RACO Agreements) within the continental United States.** **Tech Transfer and RACO Agreements are applications built on a service management platform. The platform uses self-encrypting hard drives for database servers which is FIPS 140-2 Level 2 validated. Backups are encrypted using FIPS approved ciphers. Customers do not have logical or physical access to the service management platform. Customer data is logically separated from management data through separate VLANs.** **Encryption at rest and in transit is implemented for all components of this system.**

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:
DEPT-23, Information Collected Electronically in Connection with Department of Commerce Activities, Events, and Programs
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:
DAA -0167-2016-0007 (rNIS) **DAA-GRS-2013-0003-0001 (RACO)** **NIST Records Schedule item 36 (CRADAs)** **NIST Records Schedule item 35 (patent licensing and licensed patent files)** **NIST Records Schedule item 33a (patent files)** **GRS 1.1/010 Financial management and reporting administrative records** **GRS 5.7/070 Federal register notices other than proposed and final rules** **GRS 6.5/010 Public Customer Service Records (all components)**
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 **Degaussing** **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
Quantity of PII **Obligation to Protect Confidentiality** **Access to and Location of PII**	**Quantity of PII-The majority of the information is Work-Related Data.** **Obligation to Protect Confidentiality-Obligation exists to protect confidentiality since laboratory handling of calibration results could be deemed proprietary BII.** **Access to and Location of PII-The information is Work-Related Data, and the system is located at the NIST Gaithersburg, Maryland facility within the continental United States.**

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 work related data).

Mitigating controls include employing and monitoring administrative access, training for administrators, and assurance of compliance to records management schedules. The type of data collected is minimal to only that necessary to conduct the purpose.

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

Yes, the conduct of this PIA results in required business process changes.
Explanation
The Tech Transfer and RACO Agreements components had change in the underlying technology which prompted changing business processes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

Yes, the conduct of this PIA results in required technology changes.
Explanation
The Tech Transfer and RACO Agreements components were built into a service management operating environment.