Template Version Number: 01-2021

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: Claire W. Barrett, 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

CLAIRE BARRETT Digitally signed by CLAIRE BARRETT
Date: 2024.03.25 12:38:09 -04'00' 3/25/2024

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: 100-02 Associate Directors' Staff Offices System

Introduction: System Description

Provide a brief description of the information system.

The 100-02 Associate Directors' Staff Offices System supports the day-to-day functions of the NIST Associate Directors' (AD) offices. The information processed within the components affects all elements NIST operations including strategic planning, evaluation and assessment of programmatic impact, allocation, and expenditure of resources; financial and human resource management and reporting; as well as all infrastructure support and asset management issues necessary for the operations of NIST.

The following system components contain or otherwise store, process, or transmit sensitive PII and/or BII:

- **iEdison: Helps government grantees and contractors comply with a federal law, the Bayh-Dole Act. Bayh-Dole regulations require that government funded inventions be reported to the federal agency who made the award by reporting government-funded subject inventions, patents, and utilization data via the web to the government agency that issued the funding award. It is an interagency application because it provides a single interface for grantees and contractors to interact with any participating agency.**

- **Redesigned NVLAP Information System (rNIS): Is a hybrid application with both internal and external (internet-facing) components. It is used to capture, process, and analyze data provided by laboratories applying for accreditation. The internal National Voluntary Laboratory Accreditation Program (NVLAP) program staff use rNIS to store and process the data for accreditation applications. The application supports all twenty-one (21) laboratory accreditation programs offered by NVLAP. rNIS helps manage the NVLAP accreditation process by providing the following:**
  - **A channel for laboratories to submit application documents online, and to obtain the results of the accreditation after the process is complete.**
  - **The capability to the manage application workflow and generate the reports used by NVLAP personnel in support of the NVLAP accreditation program.**
  - **An internal record of accreditation history for each lab.**
  - **The capability to generate letters that are mailed to laboratories in support of the accreditation process (i.e., reminder and expiration letters).**

Moderate impact data is stored and processed within the rNIS application. Deficiencies found during on-site assessments for laboratories are stored in rNIS. The detailed results of on-site assessments (i.e., reasons for a lab not obtaining accreditation) are stored in hard copy format within the NVLAP storage room and in the rNIS. There is also a functional Oracle account ("NVLAP_NIS") used on the backend side of the ColdFusion application. NVLAP development team uses this account occasionally for supporting the production.

- **<u>Technology Transfer ServiceNow Application:</u> Is an application in the NIST ServiceNow instance (188-01) designed to manage, track, and report on the creation, review and approval processes for Cooperative Research and Development Agreements (CRADA), Materials Transfer Agreements (MTA), Data Transfer Agreements (DTA), and Non-Disclosure Agreements (NDA), facilitate the disclosure of inventions, and facilitate, track and report on the status of Patent Applications. This application streamlines these approval and disclosure processes, and provides transparency to customers, leadership, various groups involved in the processes, and TPO.**

  The application is composed of two primary modules. One module is designed to manage the four agreement types (CRADA, MTA, DTA, NDA) and facilitate their inter-office approval via a workflow. The other module is for processing the DN-45 form (and related inventor information forms) for the disclosure of inventions and tracking progress on related patent applications.

  The primary customers for this application are NIST's scientific staff and laboratories, who require these agreements, disclosures and patent applications as a regular part of their mission-related operations. The application provides customers with an easy-to-use interface, via the ServiceNow Service Portal, to submit and manage their agreement, invention disclosure and patent application packages and maintain visibility into process status.

  The primary owners of these processes are TPO and the Office of Chief Counsel. The TPO is the product owner of the ServiceNow Technology Transfer Application in the NIST instance. The ServiceNow Technology Transfer Application provides these process owners with a workflow that coordinates the review of these agreements; a shared document repository; the means to communicate openly with each other and with customers, and performance data support informed decision-making.

  Tech Transfer's use of the DN-45 Form: The Business Identifiable Information (BII) in Section 6.1 of the NIST DN-45 form for the foreign entities is only applicable when there is an inventor that is not a U.S. citizen. In this case, the foreign person would be an inventor and would know the information as they are a co-owner. This would give them access only to their own inventions reported in the system. Contact information is collected in the case of patents since they will be part of a legal proceeding. The BII collected for reported inventions is

moderate until it can be filed. For collaboration agreements, the scope is BII and proprietary to the partner. These are protected from the Freedom of Information Act (FOIA) as proprietary information and under 35 U.S. Code 205 prior to invention filing.

a) *Whether it is a general support system, major application, or other type of system*
The component(s) are part of the 100-02 Associate Directors' Staff Offices System, which is a General Support System (GSS).

b) *System location*
The component(s) of the 100-02 Associate Directors' Staff Offices System is/are located as follows:

- **<u>iEdison:</u> Is located in the NIST AWS East and at the NIST Gaithersburg campus.**
- **<u>Redesigned NVLAP Information System (rNIS):</u> Is located at the NIST Gaithersburg campus.**
- **<u>Technology Transfer ServiceNow Application:</u> Is in a data center 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 100-02 Associate Directors' Staff Offices System component are standalone but relies on the NIST infrastructure.

d) *The way the system operates to achieve the purpose(s) identified in Section 4*
The 100-02 Associate Directors' Staff Offices System components operates as follows:

- **<u>iEdison:</u> (Interagency Edison Application): Is an online reporting system for recipients of federal research agreements to report resulting inventions to the government funding agency, as required by the Bayh-Dole Act.**
- **<u>Redesigned NVLAP Information System (rNIS):</u> NIST administers the National Voluntary Laboratory Accreditation Program (NVLAP). NVLAP provides accreditation services through various laboratory accreditation programs (LAPs), which are established based on requests and demonstrated need.**
- **<u>Technology Transfer ServiceNow Application:</u> 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), Non-Disclosure Agreements (NDA), and DN-45 forms, facilitates disclosure of inventions, and facilitates, tracks, and reports on the status of patent Applications.**

e) *How information in the system is retrieved by the user*

The 100-02 Associate Directors' Staff Offices System information is retrieved as follows:

- **<u>iEdison:</u> Authorized 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 agencies and organizations may retrieve information about their own institutions' invention and patents.**

- **<u>Redesigned NVLAP Information System (rNIS):</u> 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.**

- **<u>Technology Transfer ServiceNow Application:</u> 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.**

f) How information is transmitted to and from the system

The 100-02 Associate Directors' Staff Offices System information is transmitted as follows:

- **<u>iEdison:</u> Intake is via website/web portal.**

- **<u>Redesigned NVLAP Information System (rNIS):</u> Intake is via website/web portal.**

- **<u>Technology Transfer ServiceNow Application:</u> Intake is via website/web portal.**

g) Any information sharing

The 100-02 Associate Directors' Staff Offices System information may be shared as follows:

- **<u>iEdison:</u> Case-by-Case - DOC bureaus, Case-by-Case - Federal Agencies, Case-by-Case - Foreign entities, Case-by-Case - Private Sector, Case-by-Case - Within the bureau**

- **<u>Redesigned NVLAP Information System (rNIS):</u> Case-by-Case - DOC bureaus, Case-by-Case - Federal Agencies, Case-by-Case - Private Sector, Case-by-Case - Within the bureau**

- **<u>Technology Transfer ServiceNow Application:</u> Case-by-Case - DOC bureaus, Case-by-Case - Federal Agencies, Case-by-Case - Private Sector, Case-by-Case - Within the bureau**

- **Other:**
- **Case-by-Case - DOC bureaus (Technology Transfer ServiceNow Application: NTIA; PII/BII may be shared with other bureaus if they are party to a specific agreement.)**
- **Case-by-Case - Federal Agencies (Technology Transfer ServiceNow Application: FDA, NIH; PII/BII may be shared with other agencies if they are party to a specific agreement.)**
- **Case-by-Case - Within the bureau (Technology Transfer ServiceNow Application: TPO, OCC, and relevant OU(s); rNIS: OFRM (Accounts Receivable); iEdison: When NIST is the funding Federal agency)**

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.

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, 35 U.S.C. §200; 35 U.S.C. §207.

Accreditation requirements 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.

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*
The Federal Information Processing Standards (FIPS) 199 security impact category for the system is Moderate.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing 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.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

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
Citizenship
Telephone Number
Email Address
Other general personal data:

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
DUNS Number

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
NIST inventions, patents, disclosures, agreements (iEdison) **Results of assessments performed by accreditation laboratories (rNIS)** **Intellectual property related data (e.g., patent named inventor) and any associated patent-related business endeavors (Technology Transfer ServiceNow Application)**

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains
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: 0693-0031, Customer Satisfaction **<u>iEdison</u>: 0693-0090, iEdison** **<u>Redesigned NVLAP Information System (rNIS)</u>: 0693-0003, National Voluntary Laboratory Accreditation Program (NVLAP) Information Collection System** **0693-0033, Foreign National Request Form** **<u>Technology Transfer ServiceNow Application</u>: 0693-0085, NIST Invention Disclosure and Inventor Information Collection**

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)* N/A

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)
Other:

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)* **N/A**

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. *(Check all that apply.)*

Purpose
For administrative matters **To improve Federal services online** **To promote information sharing initiatives**
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).

iEdison: Information collected is in reference to patents and inventions that are funded through Federal Government agency grants. Information is provided by Federal employees and members of academic and private institutions.

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

Technology Transfer ServiceNow Application: Information collected is in reference to federal employees and associates for administration of potential patents or collaborations.

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.**

<u>Section 6</u>: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)* **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 – Foreign entities** **Case-by-Case – Private Sector** **Case-by-Case - Within the bureau** **Other (specify) below**
Other:
Case-by-Case - DOC bureaus (Technology Transfer ServiceNow Application: NTIA; PII/BII may be shared with other bureaus if they are party to a specific agreement.) **Case-by-Case - Federal Agencies (Technology Transfer ServiceNow Application: FDA, NIH; PII/BII may be shared with other agencies if they are party to a specific agreement.)** **Case-by-Case - Within the bureau (Technology Transfer ServiceNow Application: TPO, OCC, and relevant OU(s); rNIS: OFRM (Accounts Receivable); iEdison: When NIST is the funding Federal agency)**

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities? **No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII**

6.3 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 184-12, Amazon Web Services (AWS) (iEdison) **NIST 188-01, Platform Services Division System (Technology Transfer ServiceNow Application)** **Technical controls are described in Section 8.2.**

6.4 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

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 NIST Site Privacy Policy can be found at: https://www.nist.gov/oism/site-privacy **The iEdison Privacy Act Statement can be found at https://iedison.nist.gov/iedison/agreement.xhtml** **The Technology Transfer ServiceNow Application Privacy Act Statement can be found on the internal application interface.**
The reason why notice is/is not provided:
Redesigned NVLAP Information System (rNIS): Information in this system is not retained in a Privacy Act System of Records. Although there is not a Privacy Act Statement provided, the interface shows a warning banner alerting individuals of the sensitive nature of data, and confidentiality and privacy compliance.

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:
iEdison: Yes, however, if individuals do not consent to provide PII/BII, they will not be able to enter records and fully use the system, which would be in potential violation of their award terms and conditions and Federal regulations.

Redesigned NVLAP Information System (rNIS): Yes, although a laboratory will be denied an accreditation by refusing to provide the necessary PII and/or BII, and/or by refusing to consent to particular uses as described in the NIST Handbook 150.

Technology Transfer ServiceNow Application: Yes, although the invention disclosure or collaboration/agreement process cannot commence unless the required PII and/or BII is provided.

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:
iEdison and Technology Transfer ServiceNow Application: Yes, the Privacy Act Statement (PAS) states that supplying the information is indicating consent for use. The PAS specifically states, "Furnishing this information is voluntary. When supplying this information, you are indicating your voluntary consent for NIST to use the information you submit for the purpose stated." **Redesigned NVLAP Information System (rNIS): Yes, an opportunity to consent to particular uses of work-related data is made available through the application process.**

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:
Edison: PII/BII can be updated by either the individual or Authorized User (for active records). **Redesigned NVLAP Information System (rNIS): Yes, individuals may contact their Authorized Representative who may review/update work-related data directly in the application.** **Technology Transfer ServiceNow Application: No, any PII/BII obtained is specific to the individual timebound agreement. When the agreement is expired, the PII/BII is considered expired.**

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

- **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 5 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 and privacy 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 and privacy provisions in their contracts required by DOC policy.**

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).
04/01/2024

Other administrative and technological controls for the system:

Technology Transfer ServiceNow Application uses the Attachment Application, which enables encryption of data at rest.

8.2 Provide a 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.

iEdison utilizes a web interface for customer access, with data stored in an instance of Amazon Web Services. The component does not technically or feasibly enforce PIV credential to access but does verify use of Government credentials, as applicable.

To guard against the interception of communication over the network, Redesigned NVLAP Information System (rNIS) uses the Transport Layer Security (TLS) protocol which encrypts communications for the external (internet-facing) component for the accredited laboratory's use.

Technology Transfer ServiceNow Application uses 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 Redesigned NVLAP Information System (rNIS), and Culpepper, Virginia (Technology Transfer ServiceNow Application) within the continental United States.

Technology Transfer ServiceNow Application is 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 PII/BII 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 (e.g., organizational name).

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:
iEdison and Technology Transfer ServiceNow Application: **DEPT-23, Information Collected Electronically in Connection with Department of Commerce Activities, Events, and Programs, Federal Register Citation 78 FR 42038**
SORN submission date to the Department:

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

Yes, there is an approved record control schedule.
Name of the record control schedule:
iEdison **NIST Records Schedule is under development.** **Redesigned NVLAP Information System (rNIS)** **DAA -0167-2016-0007 (rNIS)** **GRS 1.1/010 Financial management and reporting administrative records** **GRS 5.7/070 Federal register notices other than proposed and final rules** **Technology Transfer ServiceNow Application** **NIST Records Schedule item 36 (CRADAs)** **NIST Records Schedule item 35 (patent licensing and licensed patent files)** **NIST Records Schedule item 33a (patent files)**
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. *(Check all that apply.)*

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.)*

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 Indicate which factors were used to determine the above PII confidentiality impact level. *(Check all that apply.)*

Factors that were used to determine the above PII confidentiality impact levels	Explanation
Quantity of PII	**The majority of the information is Work-Related Data.**
Obligation to Protect Confidentiality	**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	**Access to and Location of PII- The information is Work-Related Data, and the component is located at the NIST Gaithersburg, Maryland facility, and/or cloud facilities as previously defined 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 users 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. Minimizing the collection of data to only that which is necessary for the purpose.**

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

Points of Contact and Signatures

Information System Security Officer or System Owner

Name: Huang, Chihming (Richard)
Phone: Not available
Email: chihming.huang@nist.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: CHIHMING HUANG Digitally signed by CHIHMING HUANG Date: 2024.03.22 15:32:43 -04'00'

Chief Information Security Officer

Name: Heiserman, Blair
Phone: 301-975-3667
Email: nist-itso@nist.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: Digitally signed by BLAIR HEISERMAN Date: 2024.03.21 17:05:23 -04'00'

Co-Authorizing Official

Name: Loftin, Bethany
Phone: 301-975-0496
Email: bethany.loftin@nist.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: BETHANY LOFTIN Digitally signed by BETHANY LOFTIN Date: 2024.03.25 09:34:59 -04'00'

Authorizing Official

Name: Sastry, Chandan
Phone: 301-975-6500
Email: chandan.sastry@nist.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: CHANDAN SASTRY Digitally signed by CHANDAN SASTRY Date: 2024.03.22 15:19:34 -04'00'

Privacy Act Officer

Name: Fletcher, Catherine
Phone: 301-975-4054
Email: catherine.fletcher@nist.gov

I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA.

Signature: CATHERINE FLETCHER Digitally signed by CATHERINE FLETCHER Date: 2024.03.21 13:12:49 -04'00'

Chief Privacy Officer

Name: Barrett, Claire
Phone: 301-975-2852
Email: claire.barrett@nist.gov

I certify that the PII/BII processed in this IT system is necessary and this PIA ensures compliance with DOC policy to protect privacy.

Signature: CLAIRE BARRETT Digitally signed by CLAIRE BARRETT Date: 2024.03.25 12:33:39 -04'00'

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.