Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
401-01 iEdison System

Reviewed by: Claire 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

CHARLES CUTSHALL Digitally signed by CHARLES CUTSHALL Date: 2025.03.26 11:42:25 -04'00' 3/26/25

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: 401-01 iEdison

Introduction: System Description

Provide a brief description of the information system.
The 401-01 iEdison (Interagency Edison Application) helps government grantees and contractors comply with 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. iEdison is an interagency application that provides a single interface for grantees and contractors to complete this required reporting and interact with participating agencies.

iEdison 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. iEdison requires the federal funding recipients and Federal agency to register for an account, and thereafter provides a web interface for its customers, storing submitted data in a backend database.

iEdison was previously hosted by the National Institutes of Health (NIH). NIST assumed responsibility for iEdison in August 2022 and was authorized under NIST System 100-02. NIST has selected to establish as a stand alone system entitled 401-01, iEdison System.

This PIA addresses NIST's functions as both a service provider for Federal agencies, and a user of iEdison for its NIST funded inventions. Federal agency customers must address their use of iEdison within their own PIA and reference their applicable System of Records Notice.

a. *Whether it is a general support system, major application, or other type of system.*
The component(s) are part of the 401-01 iEdison, which is a major application.

b. *System location.*
The components of the 401-01 iEdison are located as follows:
- **iEdison:**
  - In the NIST AWS East and at the NIST Gaithersburg campus.

c. *Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects).*
The 401-01 iEdison system is a standalone system but relies on the internal NIST infrastructure.
  - NIST 181-04, IT Security and Networking

- NIST 184-12, Amazon Web Services (AWS) component

d. The way the system operates to achieve the purpose.

The 401-01 iEdison system operates as follows:

- **<u>iEdison:</u>**
  - Is a web application requiring registration, that receives, stores, tracks, sorts, monitors, and generates reports of inventions, patents, and the utilization thereof that have resulted from awards to extramural grant or contract funding recipients across more than 30 U.S. federal funding agency offices. Where annotated with "[new]", this indicates information that was not previously in iEdison when NIST assumed responsibility from NIH.

  - **Funding Recipients** can:
    - Create and submit [new] invention reports. Each [new] invention report is assigned an Extramural Invention Report (EIR) number and contains the source(s) of federal funding, and inventor name(s).
    - Securely and confidentially upload written descriptions of inventions.
    - Create [new] patent reports associated with the invention record and provide the government with a license confirming the government's use of the invention and upload any patent application or issued patent with acknowledgment of government support.

  - **General iEdison Users** can:
    - Access invention, patent, and utilization information regarding their own institutions' inventions and patents, including those submitted to the NIH sponsored version of iEdison. All records maintained by NIH were imported to the NIST system in August 2022.
    - Add or modify existing data and generate reports of inventions and patents reported.
    - See a graphic overview of an invention and its related patent records.
    - Upload all aspects of invention, patent, and utilization reports needed to fully comply with reporting statutes and regulations.
    - Receive notification messages of what information is needed to complete a report and reminders of the due dates of actions that need to be taken to retain and maintain rights to an invention.

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

The 401-01 iEdison information is retrieved as follows:

- **<u>iEdison:</u>**
  - The application is a public facing application and requires authenticated role-based access to retrieve data either using the **Web iEdison** (public facing application) or an **API System Client.**

f. How information is transmitted to and from the system.

The 401-01 iEdison information is transmitted as follows:

- **<u>iEdison:</u>**

- **Web iEdison** users connect to iEdison with a supported browser using the HTTPS protocol to encrypt transmission traffic. All users are required to sign in using Login.gov prior to entering and retrieving any record in iEdison. When users enter a record, the system validates that the data entered are in the expected format and data type before saving the record to the database. Before information is transmitted to the user, the system ensures the user's permission based on the organization/agency role(s) which are stored in the database prior display of a record. If users do not have permission, an access denied message is displayed.

- A**PI System Clients** connect to the iEdison API using the HTTPS protocol to encrypt transmission traffic when entering and retrieving data. The iEdison API uses the Mutual TLS authentication where the API client must provide a valid PKI certificate from one of the NIST approved certificate Vendors. The PKI certificate must be renewed annually.

g. *Any information sharing.*

The 401-01 iEdison information may be shared as follows:

- **<u>iEdison:</u>**
  - Case-by-Case - DOC bureaus (when the bureau is the funding Federal agency)
  - Case-by-Case - Federal Agencies (when the Agency is the funding Federal agency)
  - Case-by-Case - Foreign entities (when the recipient of funds is subject to reporting requirements)
  - Case-by-Case - Private Sector (when the recipient of funds is subject to reporting requirements)
  - Case-by-Case - Within the bureau (when NIST is the funding Federal agency)
  - Other:
    - Case-by-Case - Within the bureau (for purposes of managing iEdison)

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).**

- **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; 37 U.S.C., Patents, Trademarks, and Copyrights; 35 U.S.C. 202-209 (Bayh-Dole Act); 15 U.S.C. 3710(g) (Federal Transfer Act); Executive Order 12591, Facilitating Access to Science and Technology; Executive Order 14104, Federal Research and Development in Support of**

Domestic Manufacturing and United States Jobs.

- **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
Telephone Number
Email Address
Other*
Other general personal data:
Customers of iEdison may have their own invention disclosure form(s) and/or related artifacts that may include other data types. NIST has provided guidance to customers of iEdison that data types which include General Personal Data (GPD) should be redacted prior to upload.

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 (i.e., Dunn and Bradstreet) and/or Unique Entity Identifier (UEI) 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), royalties received, licensee names, manufacturing locations

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 (to include foreign entities whom are grant recipients, cooperative agreement partners, etc.) **Private Sector**
Other:

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

When users enter a record, the system validates the data entered are in the expected format and data type before saving the record to the database. 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: 0693-0090, iEdison ***Note: Federal agency customers must address their use of iEdison within their own PIA and reference their applicable OMB Control Number(s) if any customer specific forms are utilized.***

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).

The PII/BII identified is in reference to patents and inventions that are funded through Federal Government agency grants, contracts, and cooperative agreements. Information is provided by Federal employees and members of academic and private institutions.

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.)

Insider threat: 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). **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. And information collected is limited to only that which is needed for the service.**

Section 6: 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 (when the bureau is the funding Federal agency) **Case-by-Case - Federal Agencies (when the Agency is the funding Federal agency)** **Case-by-Case – Foreign entities (when the recipient of funds is subject to reporting requirements)** **Case-by-Case – Private Sector (when the recipient of funds is subject to reporting requirements)** **Case-by-Case - Within the bureau (when NIST is the funding Federal agency)** **Other (specify) below**
Other:
Case-by-Case - Within the bureau (for purposes of managing iEdison)

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 internal NIST 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 181-04, NIST IT Security and Networking **NIST 184-12, Amazon Web Services (AWS) component** **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
Government Employees **Contractors** **Other**
Other:
Grant recipients, cooperative agreement partners, etc., whom have registered with iEdison

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 **A Privacy Act Statement is presented on the iEdison login page: https://iedison.nist.gov**
The reason why notice is/is not provided:

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:
If individuals decline 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.

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:
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."

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:
PII/BII can be updated by either the individual or Authorized User (for active records).

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 and privacy 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 (previously authorized under NIST System 100-02)
Below is the date of the most recent Assessment and Authorization (A&A).
12/15/2024 (for NIST 401-01)

Other administrative and technological controls for the system:

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 credentials to access but does verify use of Government credentials, as applicable. The application uses login.gov with multi-factor authentication (MFA) employed.

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:
DEPT-23, Information Collected Electronically in Connection with Department of Commerce Activities, Events, and Programs, 78 FR 42038 ***Note: Federal agency customers must address their use of iEdison within their own PIA and reference their applicable System of Records Notice.***
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, iEdison records are covered by an approved records control schedule.
Name of the record control schedule:

• **Recordkeeping Grant Case Files:**
  ○ GRS 1.1 **Financial Management and Reporting Records and**
  ○ GRS 1.2 **Grant and Cooperative Agreement Records**
• **User Profile Records:** GRS 3.2/30-31
• **Public Customer Service Records:** GRS 6.5/20
• **Inventions, Patents, and Utilization Data Records: (currently in legal review)**
 	
Note: NARA recommends that each agency who owns their respective data utilize GRS 1.2/030 for disposition authority.

The stage in which the project is in developing and submitting a records control schedule:
Inventions, Patents, and Utilization Data Records: (currently in legal review)
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
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 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 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.)

Insider threat: 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