Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
770-01 Information Technology Laboratory (ITL) Research System

Reviewed by: Claire Barrett, 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

TIFFANY DANIEL Digitally signed by TIFFANY DANIEL
Date: 2026.05.25 19:37:43 -04'00'

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: 770-01 Information Technology Laboratory (ITL) Research System

Introduction: System Description

Provide a brief description of the information system.

The 770-01 Information Technology Laboratory (ITL) has the broad mission to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology through research and development in information technology, mathematics, and statistics.

The system contains the following components:

- **Parent:** Provides Common Control inheritance to all subcomponents.
- **Cloud Services (AWS):** Is comprised of all projects within the 770-01 Information Technology Laboratory (ITL) Research System that leverage Amazon Web Services, cloud services. The following utilize Amazon Web Services (AWS):
    - Hosting Data Science Evaluation series which falls under the ITL Big Data portfolio for evaluation tasks.
    - Language Recognition Evaluation (LRE) and Speech Recognition Evaluation (SRE) to share data and source code.
    - Ad-hoc computational resources, host short-term web services for external customers and distribution of data sets for evaluations.
    - **Automated Cryptographic Validation Protocol (ACVP)** consists of an external public facing application residing in the NIST managed AWS cloud, and an internal processing environment that resides on the internal CSD network.
    - **National Vulnerability Database (NVD)** consists of an external public facing application residing in the NIST managed AWS cloud. The test/dev NVD environment also resides within AWS.
    - **Statistical Engineering Division (SED)** uses AWS for various applications, including Decision Tree and Abacus.
    - **Software and Systems Division (SSD)** uses AWS for Computer Forensics Reference Data Sets (CFReDS) and National Software Reference Library (**NSRL**).

- **External Facing Apps:** Encompasses all public facing applications supported within the 770-01 Information Technology Laboratory (ITL) Research System.
- **Foreign Travel Devices:** Includes devices used to support foreign travel.
- **Internal Facing Apps:** Encompasses all internal facing applications supported within the 770-01 Information Technology Laboratory (ITL) Research System.
- **Locally Managed Assets:** Low impact servers that process/store data and are locally managed.
- **Locally Managed Clients:** Desktops and laptops that process/store data and are locally managed.
- **Managed Mac Clients:** Desktops and laptops that process/store data and are locally managed.
- **Locally Managed Servers:** Collection of 770-01 internal servers that process/store Moderate impact data.
    - ***Note:*** *The supporting infrastructure has moved to AWS, and thus evaluation to decommission this component (9/30/24) is being conducted.*
- **Managed Windows Clients:** Clients and assets, including laptops and desktops for users (e.g., part of the NIST enterprise managed devices).
- **Network Printers:** Networked printers (e.g., part of the NIST enterprise managed devices).
- **Networked Devices:** Hosts firewalls and routers as well as miscellaneous equipment that requires scanning (e.g., KVM switches, docking stations, dongles, etc.).
- **Public Facing Servers:** Servers maintained either locally or managed through OISM.
- **REN Assets:** Internet of Things (IoT) laboratory and other miscellaneous equipment that reside in the Research Equipment Network (REN) to continue operation.

The following system components contain or otherwise store, process, or transmit sensitive PII and/or BII. The remainder of this PIA is scoped to these component(s):

- **Biometric Research Lab (BRL) Network:** The BRL provides the infrastructure to conduct research on various biometric modalities, engaging in national and international standards development, and testing and evaluating technology using biometrics.
- **Information Collections – Public:** The National Initiative for Cybersecurity Education (NICE) vision is to prepare, grow, and sustain a cybersecurity workforce that safeguards and promotes America's national security and economic prosperity. As part of this vision, collections of information are sought and made publicly available:

- **NICE Cybersecurity Career Ambassador Finder**
- **NICE Cybersecurity Apprenticeship Program Finder**
- **NICE Cybersecurity Career Week Event and Activity Portal**

a. Whether it is a general support system, major application, or other type of system.

The components are part of 770-01 Information Technology Laboratory (ITL) Research System, which is a General Support System (GSS).

b. System location.

The components of 770-01 Information Technology Laboratory (ITL) Research System are located as follows:

- **Biometric Research Lab (BRL) Network:** Is located at the NIST Gaithersburg, Maryland campus.
- **Information Collections – Public:** Uses computing services provided by AWS (including Acquia Cloud solution), which resides in the AWS-East region (reference NIST 183-01 Applications System Division (ASD) - Moderate Applications - WCM).

c. Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects).

The 770-01 Information Technology Laboratory (ITL) Research System components are standalone but rely on the NIST infrastructure.

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

770-01 Information Technology Laboratory (ITL) Research System component operate(s) as follows:

- **Biometric Research Lab (BRL) Network:** The BRL provides the infrastructure for software development, research, and evaluation of technologies for fingerprint matching evaluation research under the USA PATRIOT Act working with the Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS), and Intelligence Advanced Research Projects Activity (IARPA).
- **Information Collections – Public:**
  - **NICE Cybersecurity Career Ambassador Finder:** An ambassador submits their information via a web form (https://www.nist.gov/itl/applied-cybersecurity/nice/events/cybersecurity-career-week/cybersecurity-career-ambassador). The NICE Program Office receives notification via email that an entry has been received. Authorized NICE Program Office staff review entries to ensure that the submitter is an ambassador, that content is within scope, and to ensure accuracy of the submitted data (e.g., no typos or broken links).

Authorized NICE Program Office staff then approve the entry for listing on the public webpage. The webpage is reviewed annually to ensure entries are current. Staff remove entries for Ambassadors that no longer participate in the program or update entries as requested by the original submitter.

- **NICE Cybersecurity Apprenticeship Program Finder:** An Apprenticeship program owner submits information via a web form (https://www.nist.gov/form/nice-apprenticeship-program-find). The NICE Program Office receives notification via email that an entry has been received. Authorized NICE Program Office staff review entries to ensure that the content is within the scope of the program, there are no typos, and that all links are working. Authorized NICE Program Office staff then approve the entry for listing on the public webpage (https://www.nist.gov/nice/apprenticeship-finder). The webpage is reviewed annually to ensure entries are current. Staff remove entries for programs that no longer exist or update entries as requested by the original submitter. Program name and email are retained, stored in Drupal, and used only for the program office to be able to follow up with the submitter to ensure their entry is current.
- **NICE Cybersecurity Career Week Event and Activity Portal:** Events and activities are submitted via a web form (https://www.nist.gov/ccw-event-activity-portal). The NICE Program Office receives notification via email that an entry has been received. Authorized NICE Program Office staff review entries to ensure that it is within scope of the program, there are no typos, and that all links are working. Staff then approve the entry for listing on the public webpage (https://www.nist.gov/nice/ccw-events). The hosting website goes live annually in the summer then is cleared of all entries at the end of the calendar year after Cybersecurity Career Week.

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

The 770-01 ITL Research System information is retrieved as follows:

- **Biometric Research Lab (BRL) Network:**
  - There is no information retrieved from the BRL network directly and no data resides outside of the BRL Network. Gateway machines are used as the interface to the BRL Network, allowing NIST Federal employees forwarding-only accounts to their actual accounts, which are restricted to SSH to their shell accounts and RDP into the specific hosts. NIST Federal employees and contractors visually inspect biometric data through custom-developed applications. Research results are then documented.

- Federal agencies can request release/return of specific data sets after images are released to NIST through partnering research agreements, the public has access to download the data sets after registration and acceptance of terms.
- A researcher registers with their business contact information through a web application, which requires acceptance of terms of usage (e.g., research purposes). Following submission, a dynamic URL (expiring after 1 week) is returned to the requestor, allowing the requestor to download the biometric dataset (e.g., NIST Special Database 300), either in part or full.

- **Information Collections – Public:**
  - **NICE Cybersecurity Career Ambassador Finder:** The public may browse the NIST website (https://www.nist.gov/itl/applied-cybersecurity/nice/events/cybersecuritycareer-week/cybersecurity-career-ambassador) to view Ambassador listings. The public can email the members listed on the website if they are interested in connecting with an ambassador.
  - **NICE Cybersecurity Apprenticeship Program Finder:** The public may browse the NIST website https://www.nist.gov/nice/apprenticeship-finder to view and search for Apprenticeship programs (e.g., users can input a zip code, which displays a map of Template Version Number: 01-2021 3 participating Programs for a specific area). The public can then select the provided Program URL to access the Programs.
  - **NICE Cybersecurity Career Week Event and Activity Portal:** The public may browse the NIST website https://www.nist.gov/nice/ccw-events to search for events and activities (e.g., users can input a zip code, which displays a map of participating Events and Activities for a specific area). The public may then select the provided Program URL to learn more about an event or an activity.

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

The 770-01 ITL Research System information components are transmitted as follows:

- **Biometric Research Lab (BRL) Network:** Prior to data transfer (intake of data into BRL), the agencies sanitize and remove all unnecessary biographic information, such as name and date of birth, from the biometric samples. Any data provided to NIST is returned to the organization agency or destroyed according to acceptable security policies in accordance with Federal law and records retention schedules. A government-furnished information (GFI) letter or a Data Transfer Agreement (DTA) accompanies each data transfer.

- **Information Collections – Public:**
    - **NICE Cybersecurity Career Ambassador Finder:** Information is collected using a public facing web form which uses Transport Layer Security (TLS) to encrypt submission transmission.
    - **NICE Cybersecurity Apprenticeship Program Finder:** Information is collected using a public facing web form which uses Transport Layer Security (TLS) to encrypt submission transmission.
    - **NIST Cybersecurity Career Week Event and Activity Portal:** Information is collected using a public facing web form which uses Transport Layer Security (TLS) to encrypt submission transmission.

g. Any information sharing conducted by the system.

The 770-01 ITL Research System information may be shared as follows:

- **Biometric Research Lab (BRL) Network:** Data is shared with researchers who have registered in the web application and accepted terms of usage.
- **Information Collections – Public:**
    - **NICE Cybersecurity Career Ambassador Finder:** Direct Access – Public
    - **NICE Cybersecurity Apprenticeship Program Finder:** Direct Access – Public
    - **NICE Cybersecurity Career Week Event and Activity Portal:** Direct Access – Public

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.

USA PATRIOT Act, Public Law 92-544, 8 CFR 103.2 (b)(9), and Enhanced Border Security and Visa Entry Reform Act of 2002.

i. The Federal Information Processing Standard (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 not 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. *(Check all that apply.)*

Identifying Numbers (IN)
File/Case ID (ID is hashed by data provider)
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 **Gender** **Age** **Race/Ethnicity** **Other general personal data**
Other general personal data:
Biometric Research Lab (BRL) Network: **Country of origin (where pictures came from)** **Name is collected from researchers, but not associated with any biometric data. (DHS and FBI never receive name with their collections.)** **Information Collection Public:** **Biographical information**

Work-Related Data (WRD)
Occupation **Job Title** **Work Address** **Work Telephone Number** **Work Email Address**
Other work-related data:
Biometric Research Lab (BRL) Network:

***WRD is collected from researchers, but not associated with any biometric data.**

Information Collections - Public:
Company Name, Company Address, Professional Bio, Program Name, Program URL

Distinguishing Features/Biometrics (DFB)
Fingerprints
Palm Prints
Voice Recording/Signatures
Photographs/Video Recording
Scars, Marks, Tattoos
Retina/Iris Scans
Other distinguishing features/biometrics:

System Administration/Audit Data (SAAD)
User ID
IP Address
Date/Time of Access
Queries Run
ID Files Accessed
Contents of Files
Other system administration/audit data:
Biometric Research Lab (BRL) Network: ***SAAD is collected from researchers but is not associated with any biometric data.**

Other Information

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

Directly from Individual about Whom the Information Pertains
Biometric Research Lab (BRL) Network: **Online** **Information Collection Public:** **Online form**
Other:

Government Sources
Within the Bureau
Other Federal Agencies
Other:

Non-government Sources
Other
Other:
Biometric Research Lab (BRL) Network: Academic institutions (approved by NIST and host Institutional Review Boards for Human Subjects Protections)

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

Biometric Research Lab (BRL) Network:

- The integrity of BRL data sets is verified at the individual file level by using a checksum for each. In addition, when a registered requestor downloads a dataset (e.g., NIST Special Database 300), a checksum is provided such that integrity can be verified by the requestor.
- Registration data collected from researchers in the web application is collected directly from the individuals.
- All data is encrypted at rest and in transit per FIPS 140-2 requirements.

Information Collection Public:

- **NICE Cybersecurity Career Ambassador Finder:** Authorized NICE Program Office staff verify Ambassadors are current members of the Ambassador Program. Staff also verify any links provided to ensure they match described activities. Staff update/correct erroneous information.
- **NICE Cybersecurity Apprenticeship Program Finder:** Authorized NICE Program Office staff verify any links provided to ensure they match the title of the submitted program. Staff update/correct erroneous information.
- **NICE Cybersecurity Career Week Event and Activity Portal:** Authorized NICE Program Office verify any links provided to ensure they match the title of the event or activity described. Staff update/correct erroneous information.

2.4 Is the information covered by the Paperwork Reduction Act?

No, the Biometric Research Lab (BRL) Network information is not 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:
NICE Cybersecurity Career Ambassador Finder: OMB Control No. 0690-0038 **NICE Cybersecurity Apprenticeship Program Finder: Not applicable** **NICE Cybersecurity Career Week Event and Activity Portal*: OMB Control No. 0690-0038** ***Titled under Cybersecurity Career Week Commitments***

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

No

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.)*

None

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
Other
Biometric Research Lab (BRL) Network: To support the research mission **Information Collection Public:** To facilitate programmatic goals

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).

Biometric Research Lab (BRL) Network:
The BRL Network includes data from members of the public who have consented to the use of their biometrics by research partners. This data is shared with NIST for research purposes through partnering research agreements. The project's output is a dataset (e.g., NIST Special Database 300) and other research findings.

Research findings are available to the public, but they must register through the web application and agree to terms of usage (e.g., research purposes) in order to request download of the dataset. Data sets do not include identifiable information.

Information Collections - Public:
NIST tracks number of entries to determine the growth of the program, but otherwise does not analyze data submitted. Data is provided voluntarily from the public. Data is collected and shared online for informational purposes only.

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.)

Biometric Research Lab (BRL) Network:
Identification. Potential threats to privacy include identifying a subject. This threat is reduced by removing all personally identifiable information prior to sharing with NIST. This risk is further mitigated by obtaining consent from the individual through the research partner before sharing the data with NIST.

Data Misuse. There is a threat of misusing the data sets (i.e., for non-research purposes). This threat is minimized by requiring the public to register and agree to the terms of usage prior to sharing the dataset. NIST research staff are also trained annually, including on the appropriate handling of personal information. The Group Manager reminds the team of this at each meeting.

Information Collections - Public:
Web scraping. Because the information is publicly available on a website, there is a risk that the data may be scraped by bad actors and used for purposes other than the intended purpose. This risk is accepted as the information is voluntarily disclosed, and submitters are informed that the information is publicly available.

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.

Biometric Research Lab (BRL) Network:
Other (specify) below

Information Collection Public:
Public – Direct Access

Other:
Biometric Research Lab (BRL) Network: **Researchers who have accepted terms of usage are granted direct access.**

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities? **No, the bureau/operating unit does not place a limitation on re-dissemination of PII/BII shared with external agencies/entities.**

6.3 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

Biometric Research Lab (BRL) Network: Yes, this component connects with or receives information from another IT system(s) authorized to process PII and/or BII. **Information Collections - Public:** No, this component does not connect or receive information from any other IT system(s) authorized to process PII and/or BII.
The name of the IT system and description of the technical controls that prevent PII/BII leakage:
NIST 184-12, Infrastructure Services System **NIST 188-01, Platform Services Division System** **Technical controls identified 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
Biometric Research Lab (BRL) Network: **General Public** **Government Employees (and Associates)** **Contractors** **Information Collections - Public:** **General Public** **Government Employees (and Associates)**
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.

Biometric Research Lab (BRL) Network: 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.

Information Collections - Public:
Yes, notice is provided on each submission form.

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

Biometric Research Lab (BRL) Network:
The NIST Privacy Act statement and/or privacy policy can be found at https://www.nist.gov/oism/site-privacy, which is linked from the web registration application.

Information Collections - Public:
NICE Cybersecurity Career Ambassador Finder: Submission Form
NICE Cybersecurity Apprenticeship Program Finder: Submission Form
NICE Cybersecurity Career Week Event and Activity Portal: Submission Form

The reason why notice is/is not provided:

Biometric Research Lab (BRL) Network:
While the biometric images are inherently recognizable, the BRL data sets come from external sources with all other identifiable personal information removed. Therefore, NIST defers to the originating source to provide notice.

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

Biometric Research Lab (BRL) Network:
Yes, individuals have an opportunity to decline to provide PII/BII.
No, individuals do not have an opportunity to decline to provide PII/BII.

Information Collections - Public:
Yes, submitters have an opportunity to decline to provide PII/BII by not submitting their information.

The reason why individuals can/cannot decline to provide PII/BII:

Biometric Research Lab (BRL) Network:
Yes, when registering to use the BRL data sets, researchers have the opportunity to decline input of their contact information in the web registration application. However, this means they will be ineligible for downloading the requested data (e.g., NIST Special Database 300).

No, the biometric images in the BRL data sets come from external sources, so NIST defers to the originating source to provide the opportunity to decline.

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

Biometric Research Lab (BRL) Network:
No, individuals do not have an opportunity to consent to particular uses of their PII/BII.

Information Collections - Public:
Yes, submitters have an opportunity to consent to uses of their PII/BII by submitting their information.

The reason why individuals can/cannot consent to particular uses of their PII/BII:

Biometric Research Lab (BRL) Network:
No, researchers do not have the opportunity to consent to particular uses of their PII when registering through the web application.

No, the biometric images in the BRL sets come from external sources, so NIST defers to the originating source to provide the opportunity to consent to particular uses.

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

Biometric Research Lab (BRL) Network:
No, individuals do not have an opportunity to review/update PII/BII pertaining to them.

Information Collections - Public:
Yes, individuals have an opportunity to review/update PII/BII pertaining to their organization prior to submission and when publicly posted. At any time, individuals may contact **nice@nist.gov** to update their information.

The reason why individuals can/cannot review/update PII/BII:

Biometric Research Lab (BRL) Network:
No, researchers do not have the opportunity to review/update PII pertaining to them once their information is submitted through the web application page.

No, the biometric images in the BRL data sets cannot be updated, but they can be removed if the individual contacts the original source. At that point, NIST would be notified to remove the images as well.

Section 8: Administrative and Technological Controls

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

Biometric Research Lab (BRL) Network:
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 and privacy 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.

Information Collections - Public:
Staff (employees and contractors) received training on privacy and confidentiality policies and practices.

The forms are published on web sites using SSL encryption for secure encryption. The content of the forms is received (once submitted) in the form creator's secure drive/site for further review using role-based access controls.

Role-based access is provided to stage and publish information on the web site.

Reason why access to the PII/BII is being monitored, tracked, or recorded:

Access logs are kept and reviewed for anomalies.

The information is secured in accordance with FISMA requirements.

Is this a new system? No
The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements.

Date of most recent Assessment and Authorization (A&A): 4/1/2026

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).*

Biometric Research Lab (BRL) Network:
The BRL data sets are stored on servers located in Seattle, Washington, and/or at the NIST Gaithersburg, Maryland, and Boulder, Colorado, facilities within the continental United States. Access to the components is restricted by user authentication, role management, and physical access controls. Access logs are kept and reviewed for anomalies on an as needed basis. The public facing web application interface utilizes an HTTPS connection.

Information Collections - Public:
Access logs are also kept and reviewed for anomalies.

To guard against the interception of communication over the network, the submission mechanism (i.e., web form) uses the Transport Layer Security (TLS) protocol which encrypts

communications, or FIPS NIST 140-2 encrypted virtual private network technologies between organizations and the public.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

No, the PII/BII is not searchable by a personal identifier.

Biometric Research Lab (BRL) Network:
No, the PII/BII is not searchable by a personal identifier.

Information Collections - Public:
Yes, information is searchable by email address.

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."

Biometric Research Lab (BRL) Network:
No, this system is not a system of records and a SORN is not applicable.

Information Collections - Public:
Yes, this system is a system of record system and a SORN is applicable.

SORN name, number, and link:

Information Collections - Public:
COMMERCE-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 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

Yes, the records are covered by an approved records control schedule and are monitored for compliance.

Name of the record control schedule:

Biometric Research Lab (BRL) Network:
General Record Schedule 5.1/020 Non-recordkeeping copies of electronic records

NIST Record Schedule for research data:
NI-167-92-1/27B
DAA-167-2019-0001-0002 Non-selected Research Project Case Files and Research

Notebooks **Information Collections - Public:** General Record Schedule 6.5/20 and 6.4/030
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
Biometric Research Lab (BRL) Network: Overwriting Deleting **Information Collections - Public:** 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
Identifiability	**Biometric Research Lab (BRL) Network:** **The data could ultimately be used to recognize an individual; however, personal identifiable information is removed. Other information is non-sensitive Personally Identifiable Information (e.g., registration contact information).**
	Information Collections - Public: **Information types can be used to identify specific individuals and businesses; however, submissions are voluntary.**
Quantity of PII	**Biometric Research Lab (BRL) Network:** **The data, by nature, is of a significant quantity.**

Factors that were used to determine the above PII confidentiality impact levels	Explanation
Context of Use	**Biometric Research Lab (BRL) Network:** **The information is used to support the research mission of NIST.**
	Information Collections - Public: **The PII/BII is for public consumption.**
Obligation to Protect Confidentiality	**Biometric Research Lab (BRL) Network:** **Identifiable private information is removed prior to acceptance by NIST and used solely for research purposes.**
Access to and Location of PII	**Biometric Research Lab (BRL) Network:** **BRL data is stored on servers located in Seattle, Washington, and/or at the NIST Gaithersburg, Maryland, and Boulder, Colorado, facilities within the continental United States.**
Data Field Sensitivity	**Information Collections - Public:** **The PII/BII is voluntarily submitted for public consumption to highlight individuals and their careers, and to identify collaborative partners, events, and programs.**
Other	**Biometric Research Lab (BRL) Network:** **The data may include biometrics of deceased persons.**

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.)

Biometric Research Lab (BRL) Network:
Although the biometric data sets have had personal identifiable information removed, they include limited associated information about depicted subjects (e.g., demographics), which may increase the likelihood of subject re-identification.

Additionally, fingerprints, facial images, and other biometric data have the unique property of enabling re-identification without any aggregate data. However, no biometric data is collected from 770-01, so the privacy notices, consent, etc. are all outside the scope of the system.

PII collected by the system is directly from the researchers who provide non-sensitive data.

In providing the BRL data sets to researchers, downloading is only permitted after the requester accepts the terms of use that state the data will only be used for research purposes. **Information Collections - Public:** Not applicable as the intended use is for public consumption (i.e., public facing web site).

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