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

Privacy Impact Assessment
for the
770-01 ITL Research System

Reviewed by: Susannah Schiller, Bureau Chief Privacy Officer

☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Jennifer Goode 10/23/2020

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

Introduction: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

(a) Whether it is a general support system, major application, or other type of system
(b) System location
(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
(d) The way the system operates to achieve the purpose(s) identified in Section 4
(e) How information in the system is retrieved by the user
(f) How information is transmitted to and from the system
(g) Any information sharing conducted by the system
(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information
(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

The 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. In support of this mission, NIST conducts research on various biometric modalities, engaging in national and international standards development, and testing and evaluating technology using biometrics, as follows:

The Biometric Research Data (BRD) project is comprised of large biometric data sets from which identifiable private information has been removed. The data sets are collected by non-NIST entities for their own research purposes, then released to NIST through partnering research agreements. NIST uses the data sets for its own biometric research (e.g., generation of metrics, etc.). In addition, after preparation by NIST, the data is made available to researchers from the public. Researchers must accept terms of usage and provide business contact information through a web registration application before they can access the data sets.

The Facial Forensic Comparison project is comprised of biometric data sets, specifically individual facial images, collected by non-NIST entities for their own research purposes, then released to NIST through a partnering research agreement. Identifiable private information has been removed from these data sets.

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

b) System location
The BRD components (i.e., host server(s), database(s), and application) supporting the BRD are located at the NIST Gaithersburg, Maryland, and Boulder, Colorado, facilities within the continental United States, and/or Seattle, Washington. The Facial Forensic Comparison data sets are stored on a stand-alone storage system located at the NIST Gaithersburg, Maryland, facility within the continental United States.

c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
The system does not share information. However, the data is made available to researchers who have accepted terms of usage.

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

Facial Forensics Comparison: NIST Federal employees and contractors visually inspect facial images for perceptual accuracy through a custom developed application. Research results are documented.

e) How information in the system is retrieved by the user
The public has access to download the data set after registration and acceptance of terms.

f) How information is transmitted to and from the system
See description in d).

g) any information sharing conducted by the system
The system does not share information. However, the data is made available to researchers who have accepted terms of usage.

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 is **Moderate.**

Section 1: Status of the Information System

1.1 The status of this information system:

This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2017 or later).

Changes That Create New Privacy Risks (CTCNPR)
Other changes that create new privacy risks:

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated.

Identifying Numbers (IN)
File/Case ID
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:
Country of Origin (Where pictures came from)

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

Distinguishing Features/Biometrics (DFB)
Fingerprints
Palm Prints
Voice Recording/Signatures
Photographs
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:

Other Information

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

Directly from Individual about Whom the Information Pertains
Online
Other:

Government Sources
Other Federal Agencies
Other:

Non-government Sources
Other
Other:
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.

The integrity of BRD data sets are 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.

2.4 Is the information covered by the Paperwork Reduction Act?

No, the information is not covered by the Paperwork Reduction Act.
The OMB control number and the agency number for the collection:

2.5 Is there any technology used that contain PII/BII in ways that have not been previously deployed?

Yes

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

Section 3: System Supported Activities

3.1 Are there any IT system supported activities which raise privacy risks/concerns?

No

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

Activities
Other:

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated.

Purpose
Other
Other:
To support the research mission.

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 BRD project includes data from individuals who have consented to use of their biometrics to research partners. This data is shared with NIST for research purposes through partnering research agreements. The output of the project is in the form of a dataset (e.g., NIST Special Database 300), and other research findings. Research findings are available to the public. Data sets are made available to the public for research purposes. Researchers must register by submitting non-sensitive contact information and agree to terms of use (e.g., research purposes) in order to request download of the dataset.

The Facial Forensic Comparison project includes facial images from those who have released their images for research purposes. The dataset is used only by NIST Federal employees and contractors conducting research. The output is in the form of research results, which are provided to the public. NIST does not have identifying private information for these data sets.

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 are reduced as this data has identifiable private information removed prior to sharing with NIST and used for research purposes. NIST does not have identifying private information for the biometric data.

For both projects, the data sets are referential (e.g., partners have the authoritative source). NIST research staff are trained annually, which includes information on the appropriate handling of information.

Section 6: Information Sharing and Access

6.1 Will the PII/BII in the system be shared?

Yes, the PII/BII in the system will be shared

The recipients the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared.

Other (specify) below
Other:
Researchers who have accepted terms of usage will be granted direct access.

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

Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII.
The name of the IT system and description of the technical controls which prevent PII/BII leakage:
NIST 184-12, Infrastructure Services System.

6.3 Identify the class of users who will have access to the IT system and the PII/BII.

Class of Users
General Public **Government Employees** **Contractors**
Other:

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system.

Yes, notice is provided by a Privacy Act statement and/or privacy policy. **No, notice is not provided.**
The Privacy Act statement and/or privacy policy can be found at:
Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at https://www.nist.gov/public_affairs/privacy.cfm, which is linked from the web registration application. **(This answer applies to the web registration application for the BRD project.)**
The reason why notice is/is not provided:
While images are inherently recognizable, the BRD and the Facial Forensic Comparison data sets come from external sources, with identifiable private information already removed. Therefore, NIST defers to the originating source to provide notice. **(This answer applies to biometric data sets, which come from external sources with identifiable private**

information already removed.)

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. No, individuals do not have an opportunity to decline to provide PII/BII.
The reason why individuals can/cannot decline to provide PII/BII:
When registering to use the BRD dataset(s), individuals 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). (This answer applies to the web registration application for the BRD project.) While images are inherently recognizable, the BRD and the Facial Forensic Comparison data sets come from external sources with identifiable private information removed. Therefore, NIST defers to the originating source to provide an opportunity to decline. (This answer applies to biometric data sets, which come from external sources with identifiable private information already removed.)

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

No, individuals do not 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:
While images are inherently recognizable, the BRD and the Facial Forensic Comparison data sets come from external sources, with identifiable private information already removed. Therefore, NIST defers to the originating source to provide an opportunity to consent. (This answer applies to biometric data sets, which come from external sources, with identifiable privacy information already removed.)

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

No, individuals do not have an opportunity to review/update PII/BII pertaining to them.
The reason why individuals can/cannot review/update PII/BII:
While images are inherently recognizable, the BRD and the Facial Forensic Comparison data sets come from external sources, with identifiable private information already removed. Therefore, NIST defers to the originating source to provide an opportunity to review/update PII/B11 pertaining to them. (This answer applies to biometric data sets, which come from external sources, with identifiable privacy information already removed.)

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system.

Staff (employees and contractors) received training on privacy and confidentiality policies and practices. Access to the PII/BII is restricted to authorized personnel only. Access to the PII/BII is being monitored, tracked, or recorded.

The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements.

The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.

NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).

A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.

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

Below is the date of the most recent Assessment and Authorization (A&A).
04/01/2020

Other administrative and technological controls for the system:

8.2 General description of the technologies used to protect PII/BII on the IT system. *(Includes data encryption in transit and/or at rest, if applicable).*

The BRD 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.

The Facial Forensic Comparison data sets are stored on a stand-alone storage system where access is restricted by user authentication, role management, and physical access controls. Data is located at the NIST Gaithersburg, Maryland, facility within the continental United States.

Section 9: Privacy Act

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

Yes, the PII/BII is searchable by a personal identifier.

9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

Yes, this system is covered by an existing system of records notice (SORN).

SORN name, number, and link:

NIST-6, Participants in Experiments, Studies, and Surveys

SORN submission date to the Department:

Section 10: Retention of Information

10.1 Are these records are covered by an approved records control schedule and monitored for compliance?

Yes, there is an approved record control schedule.
Name of the record control schedule:
NIST Record Schedule for research data: **NI-167-92-1/27B** **NI-167-92-1/28B (for note taking)**
The stage in which the project is in developing and submitting a records control schedule:
Yes, retention is monitored for compliance to the schedule.
Reason why retention is not monitored for compliance to the schedule:

10.2 Indicate the disposal method of the PII/BII.

Disposal
Overwriting **Deleting**
Other disposal method of the PII/BII:

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

11.2 The factors that were used to determine the above PII confidentiality impact levels.

Factors that were used to determine the above PII confidentiality impact levels	Explanation
Identifiability **Quantity of PII** **Context of Use** **Obligation to Protect Confidentiality** **Access to and Location of PII** **Other**	**Identifiability: The data could ultimately be used to recognize an individual, however identifiable private information is removed. Other information is non-sensitive Personally Identifiable Information (e.g., registration contact information).** **Quantity of PII: The data by nature is of significant quantity.** **Context of Use: The information is used to support the research mission of NIST.** **Obligation to Protect Confidentiality: Identifiable private information is removed prior to acceptance by NIST and used solely**

	for research purposes. **Access to and Location of PII: The BRD 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. The Facial Forensic Comparison data is stored on local storage located at the NIST Gaithersburg, Maryland, facility within the continental United States.** **Other: 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.)

Although data sets have had identifiable private information removed, they include limited associated information about depicted subjects (e.g., demographics), which may increase the likelihood of subject re-identification. Additionally, facial images have the unique property of enabling perceived re-identification without any aggregate data. **In providing the BRD data sets to the public, downloading is only permitted after the requestor accepts terms of use that state the data will only be used for research purposes.**

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