U.S. Department of Commerce
National Institute of Standards and Technology

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

Reviewed by: Susannah Schiller, Acting, Bureau Chief Privacy Officer

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

CATRINA PURVIS Digitally signed by CATRINA PURVIS Date: 2019.11.27 11:59:32 -05'00' 10/23/2019

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

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) a general description of the information in 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 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 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. 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.

(b) a description of a typical transaction conducted on the system

- 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.

(c) 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.

(d) a citation of the legal authority to collect PII and/or BII

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.

(e) the Federal Information Processing Standard (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 a new information system.
__X__ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access	X*	h. Internal Flow or Collection	X
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): * BRD web registration application					

____ This is an existing information system in which changes do not create new privacy risks, and there is not 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)					
a. Social Security*		e. File/Case ID	X	i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport		k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	X[1]	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address		o. Medical Information	
d. Gender	X[2]	j. Telephone Number		p. Military Service	
e. Age	X[2]	k. Email Address		q. Physical Characteristics	
f. Race/Ethnicity	X[2]	l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X[2]	d. Telephone Number	X[1]	g. Salary	
b. Job Title	X[1]	e. Email Address	X[1]	h. Work History	
c. Work Address	X[1]	f. Business Associates			
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	X[2]	d. Photographs	X[2]	g. DNA Profiles	
b. Palm Prints	X[2]	e. Scars, Marks, Tattoos		h. Retina/Iris Scans	X[2]
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	X
b. IP Address	X	d. Queries Run	X	f. Contents of Files	X
g. Other system administration/audit data (specify):					

Other Information (specify)

[1] Data type captured in the registration database, which contains information about researchers who want access to biometric data bases.

[2] Data type utilized in biometric databases.

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

Directly from Individual about Whom the Information Pertains					
In Person		Hard Copy: Mail/Fax		Online	X[3]
Telephone		Email			
Other (specify):					

Government Sources					
Within the Bureau		Other DOC Bureaus		Other Federal Agencies	X[4]
State, Local, Tribal		Foreign			
Other (specify):					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify): 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?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
X	No, the information is not covered by the Paperwork Reduction Act.

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

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	X
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

[3] Source used by the registration database for the BRD project.
[4] Source used for biometric data bases

	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

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

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

X	There are not any IT system supported activities which raise privacy risks/concerns.

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 a Computer Matching Program		For administering human resources programs	
For administrative matters		To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): 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 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 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.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau			
DOC bureaus			
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			X (Researchers who have accepted terms of usage)

	The PII/BII in the system will not be shared.

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

X	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII.

	Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: • NIST 184-12, Infrastructure Services System
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 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	X*	Government Employees	X
Contractors	X		
Other (specify): *The BRD data sets are made available for research use after registration and acceptance of terms of use.			

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. *(Check all that apply.)*

	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X[5]	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.	
	Yes, notice is provided by other means.	Specify how:
X[6]	No, notice is not provided.	Specify why not: 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.

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

X[5]	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: 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).
X[6]	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: 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.

[5] This answer applies to the web registration application for the BRD project.
[6] 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.

	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
X[7]	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: 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.

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.	Specify how:
X[9]	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: 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/BII pertaining to them.

Section 8: Administrative and Technological Controls

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

	All users signed a confidentiality agreement or non-disclosure agreement.
	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only. Explanation: Access logs are kept and reviewed for anomalies on an as needed basis.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Access logs are kept and reviewed for anomalies.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 4/1/2019 ☐ This is a new system.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	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).
X	A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.

[7] This answer applies to biometric data sets, which come from external sources, with identifiable privacy information already removed..

	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include 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 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."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: NIST-6, Participants in Experiments, Studies, and Surveys
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

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.)*

X	There is an approved record control schedule. Provide the 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)

	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation: Not applicable.

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding		Overwriting	X
Degaussing		Deleting	X
Other (specify):			

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

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

X	Identifiability	Provide explanation: 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).
X	Quantity of PII	Provide explanation: The data by nature is of significant quantity.
	Data Field Sensitivity	Provide explanation:
X	Context of Use	Provide explanation: The information is used to support the research mission of NIST.
X	Obligation to Protect Confidentiality	Provide explanation: Identifiable private information is removed prior to acceptance by NIST and used solely for research purposes.
X	Access to and Location of PII	Provide explanation: 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.
X	Other:	Provide explanation: 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.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

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

X	Yes, the conduct of this PIA results in required technology changes. Explanation: In order to make the BRD data sets available to the public, it required development of a public web application interface (for registration purposes), and backend storage to host the dataset. The Facial Forensic Comparison project required development of a custom application to allow internal researchers to review/compare the images.
	No, the conduct of this PIA does not result in any required technology changes.