Version Number: 01-2019

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

Privacy Threshold Analysis
for the
770-01 ITL Research System

U.S. Department of Commerce Privacy Threshold Analysis

National Institute of Standards and Technology (NIST)

Unique Project Identifier: 770-01

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a general description (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

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 purpose that the system is designed to serve
e) The way the system operates to achieve the purpose
f) A general description of the type of information collected, maintained, use, or disseminated by the system
g) Identify individuals who have access to information on the system
h) How information in the system is retrieved by the user
i) How information is transmitted to and from the system

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

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 purpose that the system is designed to serve
The components support the research mission of NIST.

e) The way the system operates to achieve the purpose
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.

f) A general description of the type of information collected, maintained, use, or disseminated by the system
In addition to work-related data and general purpose data, biometrics are collected, maintained, used, or disseminated by the system.

g) Identify individuals who have access to information on the system
BRD: The public has access to download the data set after registration and acceptance of terms.

Facial Forensics Comparison: Only authorized NIST staff and research participants have access to information on the system.

h) 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.

i) How information is transmitted to and from the system
See description in e).

Questionnaire:

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). (Skip questions and complete certification.)

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

2. Is the IT system or its information used to support any activity which may raise privacy concerns?
   NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

Activities
Other activities which may raise privacy concerns:

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?
   As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?
   As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

   The IT system collects, maintains, or disseminates PII about:

   If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.
Provide the legal authority which permits the collection of SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

Is a PIA Required?	**Yes**

CERTIFICATION

X I certify the criteria implied by one or more of the questions above **apply** to the 770-01 ITL Research System and as a consequence of this applicability, I will perform and document a PIA for this IT system.

I certify the criteria implied by the questions above **do not apply** to the 770-01 ITL Research System and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO):

Carnahan, Lisa

Signature of SO: LISA CARNAHAN Digitally signed by LISA CARNAHAN Date: 2021.03.17 11:18:08 -04'00' Date: _____

Name of Co-Authorizing Official (Co-AO):

St Pierre, James

Signature of Co-AO: JAMES ST PIERRE Digitally signed by JAMES ST PIERRE Date: 2021.03.17 19:46:58 -04'00' Date: _____

Name of Information Technology Security Officer (ITSO):

Heiserman, Blair

Signature of ITSO: Digitally signed by BLAIR HEISERMAN Date: 2021.03.10 13:01:36 -05'00' Date: _____

Name of Authorizing Official (AO):

Sastry, Chandan

Signature of AO: CHANDAN SASTRY Digitally signed by CHANDAN SASTRY Date: 2021.03.10 13:08:37 -05'00' Date: _____

Name of Privacy Act Officer (PAO):

Fletcher, Catherine

Signature of PAO: CATHERINE FLETCHER Digitally signed by CATHERINE FLETCHER Date: 2021.03.26 15:01:33 -04'00' Date: _____

Name of Acting Bureau Chief Privacy Officer (BCPO):

Wilkinson, Matt

Signature of Acting BCPO: MATTHEW WILKINSON Digitally signed by MATTHEW WILKINSON Date: 2021.04.09 13:00:01 -04'00' Date: _____