Version Number: 01-2019

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

Privacy Threshold Analysis
for the
730-01 EL Managed Infrastructure
Disaster & Failure Studies Program

U.S. Department of Commerce Privacy Threshold Analysis

National Institute of Standards and Technology (NIST)

Unique Project Identifier: 730-01

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 Engineering Laboratory Managed Infrastructure System (730-01) is using a major application to support the disaster and community resilience mission.**

b) *System location*
The primary component is located at the NIST Gaithersburg, Maryland and Boulder, Colorado facilities within the continental United States. Cloud storage services are located in Mountainview, California and in Redwood City, California. The cloud content management and file sharing service is headquartered in Redwood City, California.

c) *Whether it is a standalone system or interconnects with other systems (identifying and*

describing any other systems to which it interconnects)
The component does not share information with other internal NIST business units but utilizes NIST infrastructure services (NIST System 188-01).

d) *The purpose that the system is designed to serve*
The purpose of the disaster and failure studies mission component is to collect information that supports investigations and studies of: fire, earthquakes, high winds, errors in design and construction, flaws in materials, and even terrorist attack attacks. Central to the investigations are: (1) establishing the likely technical factor or factors responsible for the damage, failure, and/or successful performance of buildings and/or infrastructure in the aftermath of a disaster or failure event; (2) evaluating the technical aspects of evacuation and emergency response procedures that contributed to the extent of injuries and fatalities sustained during the event; (3) determining the procedures and practices that were used in the design, construction, operation, and maintenance of the buildings and/or infrastructure; (4) recommending, as necessary, specific improvements to standards, codes, and practices as well as any research and other appropriate actions based on study findings.

e) *The way the system operates to achieve the purpose*
Information is collected from various sources (i.e., other agencies and the general public), reviewed, curated, and enhanced with metadata (if necessary). The information is stored in a searchable library for subsequent analysis.

f) *A general description of the type of information collected, maintained, used, or disseminated by the system*
The survey and collection of field performance data, including photographs, video, and/or audio recordings (from individual interviews), log files, sensor data files, or technical drawings and documentation. The content of the information includes the wind environment and technical conditions associated with deaths and injuries; the performance of representative critical buildings, and designated safe areas in those buildings, including their dependence on lifelines; and the performance of emergency communications systems and the public's response to such communications.

g) *Identify individuals who have access to information on the system*
Information in the component is only accessible to: limited/authorized administrators, limited/authorized NIST curation team, authorized NIST staff and authorized partnering agency staff.

h) *How information in the system is retrieved by the user*
Information in the component is not retrievable by the submitter. Information in the component is only retrieved by authorized NIST staff and authorized partnering agency staff.

i) *How information is transmitted to and from the system*
The public submits data through a public facing interface. In addition, staff in the field collect data from the public through various authorized collection means. Exchange of

other agency data is collected in the field, on-site, or submitted directly to NIST. Hardcopy information is digitized, where possible, and comingled with other information and stored in a searchable official collection, for subsequent analysis. Hardcopy information that is not digitized is stored internally at NIST.

Questionnaire:

1. The status of this information system:
   This is an existing information system with changes that create new privacy risks.

Changes That Create New Privacy Risks (CTCNPR)
New Public Access **Internal Flow or Collection**
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.
   Yes

Activities
Audio recordings **Video surveillance** **Other**
Other activities which may raise privacy concerns:
*** Individuals may submit video footage taken both during and after an event.**

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.)."
   No, this IT system does not collect any BII.

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."
   Yes, the IT system collects, maintains, or disseminates PII.

   The IT system collects, maintains, or disseminates PII about:
   Members of the public

   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?

No, the IT system does not collect, maintain, or disseminate 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?

Yes, the sy**stem collects, maintains, or disseminates 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.

No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

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 730-01 EL Managed Infrastructure 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 730-01 EL Managed Infrastructure and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO):

Joannie Chin

Signature of SO: JOANNIE CHIN Digitally signed by JOANNIE CHIN Date: 2020.04.20 13:07:11 -04'00' Date: ____________

Name of Information Technology Security Officer (ITSO):

K. Robert Glenn

Signature of ITSO: KENNETH GLENN Digitally signed by KENNETH GLENN Date: 2020.04.20 10:11:41 -04'00' Date: ____________

Name of Privacy Act Officer (PAO):

Catherine Fletcher

Signature of PAO: CATHERINE FLETCHER Digitally signed by CATHERINE FLETCHER Date: 2020.04.28 16:55:36 -04'00' Date: ____________

Name of Co-Authorizing Official (AO):

Howard Harary

Signature of Co-AO: HOWARD HARARY Digitally signed by HOWARD HARARY Date: 2020.04.20 16:24:49 -04'00' Date: ____________

Name of Co-Authorizing Official (AO):

Chandan Sastry

Signature of Co-AO: CHANDAN SASTRY Digitally signed by CHANDAN SASTRY Date: 2020.04.29 08:57:18 -04'00' Date: ____________

Name of Bureau Chief Privacy Officer (BCPO):

Susannah Schiller

Signature of BCPO: SUSANNAH SCHILLER Digitally signed by SUSANNAH SCHILLER Date: 2020.04.10 11:28:49 -04'00' Date: ____________