

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



**Privacy Impact Assessment
for the
730-01 EL Managed Infrastructure**

Reviewed by: Matt Wilkinson, 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

Lisa Martin

for Dr. Jennifer Goode

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer

05/24/2021

Date

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

Unique Project Identifier: 730-01

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*

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

The purpose of the disaster and failure studies mission component is to collect information that supports research and 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) 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, authorized contractors, and authorized partnering agency staff. Once submitted, data is reviewed through the NIST curation process, and anonymized (if necessary) before inclusion in the official collection for research and analysis

f) 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.

g) Any information sharing conducted by the system

The component only shares information with other internal NIST business units and DOC bureaus on a case-by-case basis. The component utilizes NIST infrastructure services (NIST System 188-01).

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.

National Construction Safety Team (NCST) Act (Public Law 107-231)

National Windstorm Impact Reduction Act (Public Law 114-52)

National Earthquake Hazard Reduction Act (Public Law 95-124)

*i) The Federal Information Processing Standards (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)
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
Personal and/or business email address
Other general personal data:

Work-Related Data (WRD)
Other work-related data:

Distinguishing Features/Biometrics (DFB)
Voice Recording/Signatures
Photographs
Other distinguishing features/biometrics:

System Administration/Audit Data (SAAD)
Other system administration/audit data:

Other Information
The data collected varies depending on the nature of the disaster or failure. Names, voice recording/signatures, and photographs are most common, but each event has the potential to collect other types of incidental PII (e.g., house number, license plate, etc.). However, everything collected is strictly for

the purpose of the mission (e.g. study the disasters, structural failures, etc.). Information deemed to be PII will go through a curation process.

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

Directly from Individual about Whom the Information Pertains
In Person Telephone Hard Copy - Mail/Fax Email Online
Other:

Government Sources
Within the Bureau State, Local, Tribal Other DOC Bureaus Other Federal Agencies
Other:

Non-government Sources
Public Organizations Private Sector
Other:

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

Submitted information is reviewed for relevance and appropriateness. If necessary, information is supplemented with geographic and other related information such as metadata. Information that is deemed irrelevant or inappropriate is disposed of from the official collection.

2.4 Is the information 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:
OMB Control Number: 0693-0078.

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

No

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

Section 3: System Supported Activities

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

Yes

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

Activities
Audio recordings
Other
Other:
Individuals may submit video footage taken both during and after an event.

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:
Information being collected for (i) investigative purposes (e.g., technical causes of building failures) and for (ii) research purposes (e.g., analysis). Access is limited to authorized users following the collection. NIST's best practice is not to collect, nor maintain, unnecessary data, and methods of collection vary.

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).

Information collected is about people impacted by the disaster, including: members of the public, first responders, government officials (federal, state, and local), and other stakeholders. Information is collected by: individuals associated with federal, state, or local government, NIST hired contractors, and academic collaborators.

The information is collected for the development of findings and recommendations that will accomplish the following: (i) by understanding the technical causes leading to structural failures and then making that information public, NIST engineers and researchers strive to prevent similar failures in the future; (ii) studies conducted by NIST have led to significant changes in practices, standards, and codes to enhance the health and safety of the American public.

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 privacy threats include obtaining irrelevant information during collection of affected persons. Potential threats to privacy include images that identify locations or people. The curation process minimizes the use of this information in the official collection. A related threat to privacy is that individuals may not have the opportunity to consent as they are incidental to the collection.

Controls to minimize this include: interagency agreements, mandatory training for NIST investigators, data handling and review processes, access controls, data loss prevention, encryption of data in transit and at rest, requiring people to provide consent regarding copyright and ownership of submission in web portal.

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.

Case-by-Case - DOC bureaus
Case-by-Case - Within the bureau

Other:

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:
--

The system connects with NIST 188-01, Platform Services Division System. To prevent PII/BII leakage, FIPS validated encryption is employed for data-at-rest, access logs are kept and reviewed for anomalies, and continuous monitoring performed to maintain its annual FedRAMP authorization status.

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

Class of Users

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.

No, notice is not provided pursuant to a system of records notice published in the Federal Register.

Yes, notice is provided by a privacy policy from the online submission portal.

No, notice is not provided.

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

https://www.nist.gov/privacy-policy

The reason why notice is/is not provided:

Individuals are presented with a link to the NIST privacy policy when using the online submission portal.
--

Individuals are presented a notice when NIST engages its subpoena authority authorized by NCST. Such notice varies depending on each case whereby enactment of subpoena authority would be necessary.

Individuals are not presented a notice by NIST when PII collection is incidental to information collected by the first responders in affected areas. However, notice may be provided by other organizations collecting information in affected areas. In this case, NIST defers to the collecting agency.

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:

Individuals have opportunity to decline providing their PII by choosing not to submit information through the online submission portal, or they may decline participation in a survey, interview, or other collection.

Individuals do not have opportunity to decline providing their PII when it is incidental to information collected by the first responders in affected areas. All PII data will, however, be reviewed through a NIST curation process.

Individuals do not have opportunity to decline providing their PII when NIST engages its subpoena authority authorized by NCST.

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:

Individuals have opportunity to consent to uses of their PII when providing through the online submission portal, or they may decline submission and/or participation in a survey, interview, or other collection.

Individuals do not have opportunity to consent to using their PII when it is incidental to information collected by the first responders in affected areas. All PII data will, however, be reviewed through a NIST curation process.

Individuals do not have opportunity to consent to uses of their PII when NIST engages its subpoena authority authorized by NCST.

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:

Individuals have opportunity to review/update their PII before submission through the online portal. Once submitted, individuals may immediately reach out to eldst@nist.gov to identify concerns with a submission.

Individuals do not have opportunity to review/update their PII when it is incidental to information

collected by the first responders in affected areas. All PII data will, however, be reviewed through a NIST curation process.

Individuals do not have opportunity to review/update their PII when NIST engages its subpoena authority authorized by NCST.

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.

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.

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

An audit log is used.

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).

04/30/2020

Other administrative and technological controls for the system:

The NIST curation process reviews submitted/received data for PII, and anonymizes and/or removes PII (if necessary) prior to becoming part of the official collection for research/analysis.

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 technologies vary depending on the mission. Generally, data is protected at the FIPS-199 baseline of moderate for confidentiality.

The following technologies are used to protect PII/BII: auditing configuration, proper banners, anti-virus and patching, data loss prevention, user account management. FIPS validated encryption in transit and full disk encryption at rest exists to protect information.

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.

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."

No, this system is not a system of records and a SORN is not applicable.

SORN name, number, and link:

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:

DAA-0167-2019-0001/1.2 Non-selected Research Project Case Files and Research Notebooks: Cutoff annually at the close of the project. Destroy 15 years after cutoff, but longer retention is authorized if required for business use.

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

Shredding

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 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 Data Field Sensitivity Context of Use Obligation to Protect Confidentiality Access to and Location of PII Other	<p>Identifiable: Information could render individuals identifiable (e.g., photograph of affected residential area with persons standing nearby, or information documented in interview notes that could include other identifiable information).</p> <p>Quantity of PII: Information from other agencies combined with public collection has the potential to be a large volume.</p> <p>Data Field Sensitivity: The collection limits the PII collected to that of the submitter and information about affect persons (during interview and metadata associated with photographs or videos).</p> <p>Context of Use: The collection is for investigative and research purposes (e.g., analysis).</p> <p>Obligation to Protect Confidentiality: The goal is to study the disasters, structural failures, etc. depending on the mission requirements. All PII collected is incidental and will go through curation process. As required by: 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; National Construction Safety Team (NCST) Act (Public Law 107-231); National Windstorm Impact Reduction Act (Public Law 114-52); and National Earthquake Hazard Reduction Act (Public Law 95-124).</p> <p>Access to and Location of PII: Information will be hosted in cloud storage.</p> <p>Other: Information received from other agencies relies upon agreements with those agencies, and their acquisition of notice/consent, except incidental PII which would then engage the NIST curation process.</p>

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.)

Information being collected for (i) investigative purposes (e.g., technical causes of building failures) and for (ii) research purposes (e.g., analysis). Access is limited to authorized users following the collection. NIST's best practice is not to collect, nor maintain, unnecessary data, and methods of collection vary.
--

- 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