

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



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

Reviewed by: \_\_\_\_\_, 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

---

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: 730-01**

**Introduction: System Description**

*Provide a brief description of the information system*

**The Engineering Laboratory (EL) promotes U.S. innovation and industrial competitiveness in areas of critical national priority by anticipating and meeting the measurement science and standards needs for technology-intensive manufacturing, construction, and cyber-physical systems in ways that enhance economic prosperity and improve the quality of life.**

**The 730-01 EL Managed Infrastructure System supports the EL mission by providing a platform-independent infrastructure that supports heterogeneous file sharing, authentication, application development and support, data management, specialized research technology and support for that technology, hosting of public research applications, and security to enable the staff and guest workers of the Engineering Laboratory to focus on mission-related activities instead of IT and software development problems and solutions.**

**The following system component contains or otherwise stores, processes, or transmits sensitive PII and/or BII:**

- **Moderate Cloud Services: Cloud services authorized for the EL - Disaster and Failure Studies Program Data. Box and Google Drive storage for all Disaster and Failure studies data. Includes the Box for Google Workspace integration tool and other approved Google tools such as Contacts, Calendar, and Sites. These data come from reconnaissance and investigation efforts authorized under the National Construction Safety Team (NCST) Act and National Windstorm Impact Reduction Program (NWIRP) Act.**

**The purpose of the Disaster and Failure Studies (DFS) 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.

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

The component is part of 730-01 EL Managed Infrastructure System, which is a General Support System (GSS).

b) *System location.*

The component of 730-01 EL Managed Infrastructure System are located as follows:

**Moderate Cloud Services:** The data associated with the Disaster and Failure Studies (DFS) program resides in Google and Box cloud services and on-premises servers on the Gaithersburg, Maryland campus.

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

The 730-01 EL Managed Infrastructure System component is standalone but relies on the NIST infrastructure.

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

The 730-01 EL Managed Infrastructure System component operate(s) as follows:

**Moderate Cloud Services:** DFS 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.

The NIST-created Data Submission Portal is a tool to allow the public, first responders, and others to share data with NIST investigations. The tool requires submission of a Google form, allowing the submitter to claim ownership of the data and assign rights to NIST. Once submitted, a Box link is provided to the submitter to then upload their data, which is typically in the form of photos or videos. The submitter has 1-hour to make any changes to uploaded data. Thereafter, the submitter no longer has access to edit or view uploaded data. Submitted information is reviewed for relevance and appropriateness using procedures developed by DFS for curating data. 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.

e) *How information in the system is retrieved by the user*

The 730-01 EL Managed Infrastructure System information is retrieved as follows:

- **Moderate Cloud Services:** The submitter has 1-hour to make any changes to data uploaded through the Data Submission Portal. Thereafter, the submitter no longer has access to edit or view their uploaded data. NIST employees and associates (i.e., contractors), and authorized partnering organizations access the data using the Google and Box interfaces. Permissions are granted to folders on an as-needed basis by the principal investigators.

f) *How information is transmitted to and from the system*

The 730-01 EL Managed Infrastructure System component information is transmitted as follows:

**Moderate Cloud Services:** The public submits data through a public facing interface, the Data Submission Portal. 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 co-mingled with other information and stored in a searchable collection in Box and Google, for subsequent analysis. Hardcopy information that is not digitized is stored internally at NIST.

g) *Any information sharing*

The 730-01 EL Managed Infrastructure System information may be shared as follows:

**Moderate Cloud Services:**

Information sharing occurs using the Box and Google sharing interfaces. Official collaborators for an investigation are granted access to upload folders or working folders depending on their role in the investigation.

- Case-by-Case - DOC bureaus
- Case-by-Case - Federal Agencies
- Case-by-Case - State, local, tribal gov't agencies
- Case-by-Case – Contractors

The component shares information (through authorized access) with the NIST Library (135-01) as they are responsible for the curation process; however, no data is stored on their system. NIST infrastructure services are also utilized.

- Case-by-Case - Within the bureau:

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*

**The Federal Information Processing Standards (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 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).**

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

## **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.)*

<b>Identifying Numbers (IN)</b>
<b>Other identifying numbers:</b>
<b>Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:</b>

<b>General Personal Data (GPD)</b>
<b>Name</b> <b>Gender</b> <b>Age</b> <b>Race/Ethnicity</b> <b>Home address</b> <b>Telephone number</b> <b>Email Address</b> <b>Medical information provided by third parties (e.g., first responders, insurance companies)</b> <b>Other</b>
<b>Other general personal data:</b>
<b>Death certificates provided by third parties (e.g., hospitals in the disaster area)</b> <b>Insurance claims provided by third parties (e.g., first responders, insurance companies)</b>

<b>Work-Related Data (WRD)</b>
<b>Occupation</b> <b>Work Address</b> <b>Work Telephone number</b> <b>Work Email Address</b>
<b>Other work-related data:</b>

<b>Distinguishing Features/Biometrics (DFB)</b>
<b>Voice/Audio Recording</b>

<b>Video Recording</b> <b>Signatures</b> <b>Photographs</b> <b>Other</b>
Other distinguishing features/biometrics:
<b>Cell phone or computer images</b>

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

<b>Other Information</b>
<b>The data collected varies depending on the nature of the disaster or failure. Names, Voice/Audio Recording, Signatures, and Photographs are most common, but each event has the potential to collect other types of PII (e.g., house number, license plate, etc.). However, all information collected is strictly for the purpose of the mission (e.g., study the disasters, structural failures.).</b>

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

<b>Directly from Individual about Whom the Information Pertains</b>
<b>In Person</b> <b>Telephone</b> <b>Hard Copy - Mail/Fax</b> <b>Email</b> <b>Online (i.e., Data Submission Portal)</b>
Other:

<b>Government Sources</b>
<b>Within the Bureau</b> <b>State, Local, Tribal</b> <b>Other DOC Bureaus</b> <b>Other Federal Agencies</b>
Other:

<b>Non-government Sources</b>
<b>Public Organizations (e.g., first responders)</b> <b>Private Sector (e.g., insurance companies or hospitals)</b> <b>Universities</b> <b>Public</b>
Other:

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

<b>Submitted information is reviewed for relevance and appropriateness using procedures</b>
---

**developed by DFS for curating data. 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 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

**No**

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

Other:

### **Section 3: System Supported Activities**

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

**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. *(Check all that apply.)*

**Purpose**

**Other**

Other:

**To support the disaster and failure studies 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).



**Information collected is about a specific disaster under investigation and may include information about people impacted during the disaster including members of the public, first responders, government officials (federal, state, and local), and other stakeholders.**

**Information is collected by the public, individuals associated with federal, state, or local government, NIST employees and associates (i.e., contractors), and academic collaborators.**

**The information is collected for the development of findings and recommendations that 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.)

**Identification: Potential privacy threats include obtaining irrelevant information during collection of affected persons. Potential threats to privacy include images or video that identify locations or people, device images that contain an individual's PII.**

**Consent: Individuals may not have the opportunity to consent because data is collected and provided to NIST by third-party organizations.**

**To minimize potential privacy threats, submitted information is reviewed for relevance and appropriateness using procedures developed by DFS for curating data. Additional actions include interagency agreements, mandatory training for NIST investigators, access controls, data loss prevention, encryption of data in transit and at rest, requiring submitters to provide consent regarding copyright and ownership of material submitted in the Data Submission Portal.**

## **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.)*

**Yes, the PII/BII in the system is shared but limited to official collaborators with formal data sharing agreements. Data is only shared as part of an investigation.**

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**

<b>Case-by-Case - Federal Agencies</b> <b>Case-by-Case - State, local, tribal gov't agencies</b> <b>Case-by-Case - Within the bureau</b> <b>Case-by-Case - Contractors</b> <b>Other (specify) below</b>
Other:
<b>Case-by-Case - Within the bureau</b>

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

**No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.**

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

<b>Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII.</b>
The name of the IT system and description of the technical controls which prevent PII/BII leakage:
<b>NIST 188-01, Platform Services Division System</b>

6.4 Identify the class of users who will have access to the IT system and the PII/BII. (*Check all that apply.*)

<b>Class of Users</b>
<b>Government Employees</b>
<b>Contractors</b>
<b>Other</b>
Other:
<b>Official collaborators with formal data sharing agreements (e.g., Miami Dade Police Department, specific universities with sharing agreements, other federal agencies)</b>

## **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.

<b>Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.</b>
<b>Yes, notice is provided by a Privacy Act statement and/or privacy policy.</b>
<b>No, notice is not provided.</b>
The Privacy Act statement and/or privacy policy can be found at:
<b><a href="https://www.nist.gov/oism/site-privacy">https://www.nist.gov/oism/site-privacy</a></b>
<b><a href="https://pages.nist.gov/disaster-failure-studies-portal/form.html">https://pages.nist.gov/disaster-failure-studies-portal/form.html</a></b>
The reason why notice is/is not provided:
<b>Individuals are presented with a Privacy Act Statement and/or link to the NIST site privacy policy when using the Data Submission Portal.</b>

**Individuals are presented a notice when NIST engages its subpoena authority authorized by NCST.**

**Individuals are not presented a notice by NIST when PII collection is from a third-party organization. However, responsibility for notice resides with the collecting organization 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 data submission portal, or they may decline participation in a survey, interview, or other collection.**

**Individuals do not have opportunity to decline providing their PII to NIST when it is collected by a third-party organization. The responsibility for providing an opt-out is the responsibility of the collecting organization. All PII data is, however, reviewed through a documented 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 data 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 collected by a third-party organization. The consent process is the responsibility of the collecting organization. All PII data is, however, reviewed through a documented 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.

**Yes, 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 1-hour to update or remove their uploaded content through the Data Submission Portal. Thereafter, they do not have the opportunity to modify their submission through the Data Submission Portal.**

**Individuals do not have the opportunity to review/update their PII when it is collected by a third-party organization. Updates to collecting information reside with the original collecting organization. All PII data is, however, reviewed through a documented 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. *(Check all that apply.)*

- **Staff (employees and contractors) received training on privacy and confidentiality policies and practices to ensure that researchers know when they are handling data containing potential PII.**
- **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 moderate or higher.**
- **NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 5 recommended security and privacy 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 and privacy 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 and privacy provisions in their contracts required by DOC policy.**
- **Tagging is used in Box to identify individual data that may contain PII.**

**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).**

**04/30/2024**

Other administrative and technological controls for the system:

- 8.2 Provide a 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 are protected at the FIPS-199 baseline of moderate for confidentiality even if some of the data are low.**

**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 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

**Yes, there is an approved record control schedule.**

Name of the record control schedule:

**DAA-0167-2019-0001-0002 Non-selected Research Project Case Files and Research Notebooks.**

**The records are to be destroyed 15 years after close of the project.**

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. *(Check all that apply.)*

<b>Disposal</b>
<b>Shredding</b>
<b>Deleting</b>
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 Indicate which factors were used to determine the above PII confidentiality impact level. *(Check all that apply.)*

Factors that were used to determine the above PII confidentiality impact levels	Explanation
<b>Identifiability</b>	<b>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).</b>
<b>Quantity of PII</b>	<b>Information from other agencies combined with public collection has the potential to be a large volume.</b>
<b>Data Field Sensitivity</b>	<b>The collection limits the PII collected to that of the submitter and information about affected persons (during interview and metadata associated with photographs or videos).</b>
<b>Context of Use</b>	<b>The collection is for investigative and research purposes (e.g., analysis).</b>
<b>Obligation to Protect Confidentiality</b>	<b>The goal is to study the disasters, structural failures, etc. depending on the mission requirements. All PII collected is reviewed through curation process.</b>
<b>Access to and Location of PII</b>	<b>Information hosted in cloud storage.</b>
<b>Other</b>	<b>Information received from other agencies relies upon agreements with those agencies, and their acquisition of notice/consent.</b>

## **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 is used for:**

- (i) Investigative purposes (e.g., technical causes of building failures) and**
- (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.**

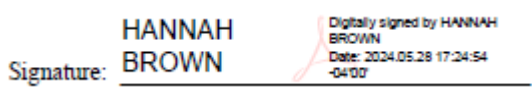
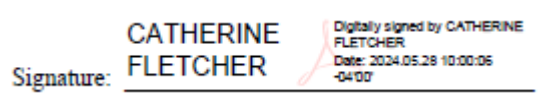
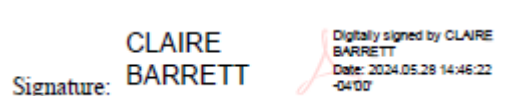
Explanation

- 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

## Points of Contact and Signatures

<p><b>Information System Security Officer or System Owner</b></p> <p>Name: Averill, Jason  Phone: 301-975-2585  Email: jason.averill@nist.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature: _____</p>	<p><b>Chief Information Security Officer</b></p> <p>Name: Heiserman, Blair  Phone: 301-975-3667  Email: nist-itso@nist.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature: _____</p>
<p><b>Co-Authorizing Official</b></p> <p>Name: Chin, Joannie  Phone: 301-975-6815  Email: joannie.chin@nist.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature: _____</p>	<p><b>Authorizing Official</b></p> <p>Name: Brown, Hannah  Phone: 301-975-2300  Email: hannah.brown@nist.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <div style="text-align: right; margin-top: 20px;">  </div>
<p><b>Privacy Act Officer</b></p> <p>Name: Fletcher, Catherine  Phone: 301-975-4054  Email: catherine.fletcher@nist.gov</p> <p>I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA.</p> <div style="text-align: right; margin-top: 20px;">  </div>	<p><b>Chief Privacy Officer</b></p> <p>Name: Barrett, Claire  Phone: 301-975-2852  Email: claire.barrett@nist.gov</p> <p>I certify that the PII/BII processed in this IT system is necessary and this PIA ensures compliance with DOC policy to protect privacy.</p> <div style="text-align: right; margin-top: 20px;">  </div>

**This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.**