Privacy Threshold Analysis
for the
Grants Management Information System (GMIS) (142-01)
U.S. Department of Commerce Privacy Threshold Analysis

Unique Project Identifier: 142-01

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 of the information system in a way that a non-technical person can understand.
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).

The Grant Management Information System (GMIS) enables a standard business process and workflow to review, select, award, and administer all NIST-issued grants and cooperative agreements.

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

b) System location
   The system is 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)

   GMIS production and test applications have interconnection to the Department of Commerce DataByDesign Grants Notification System (DBD GNS). The interconnection between GMIS and DBS GNS is two-way and always initiated by GMIS.

   In addition, GMIS has an interconnection to the Department of Health and Human Services (HHS) Grants.Gov application to retrieve grant packages. The interconnection between HHS Grants.Gov is two-way and always initiated by GMIS.

d) The purpose that the system is designed to serve
   The purpose of GMIS is to support grants administration.
e) The way the system operates to achieve the purpose
GMIS is used as the means of reviewing, selecting, awarding, and administering all issued grants and cooperative agreements administered by the NIST Grants Management Division (GMD).

f) A general description of the type of information collected, maintained, use, or disseminated by the system
The type of business identifiable information or personally identifiable information includes: identifying numbers, general personal data, work-related data, and system administration/audit data.

g) Identify individuals who have access to information on the system
NIST and DOC employees/contractors, and grant reviewers.

h) How information in the system is retrieved by the user
NIST internal users access the CBS Portal logon page HTTPS://portal.cbs.nist.gov and log into the CBS Portal application (covered in SSP 162-01). From the CBS Portal application tab, the users select GMIS. This is done from their desktop systems via the NIST Network Infrastructure using Transport Layer Security (TLS) 1.2.

Access to GMIS by OS, NTIA and OIG customers is via the DoC TLS network to the Herbert C. Hoover Building (HCHB) in Washington, D.C. – external bureau users are authenticated by their home bureau. All external traffic is encrypted using TLS 1.2. External users then access the CBS Portal logon page and GMIS in the same way as internal users.

i) How information is transmitted to and from the system
All GMIS user sessions are via TLS 1.2 at a minimum. TLS is enforced by the CBS/GMIS F5 LTM's.

GMIS transmits data to DBD GNS and the Grants.Gov using TLS 1.2 encrypted web services running on OISM application servers in the NIST data center.

Questionnaire:

1. What is the status of this information system?

   ___ This is a new information system. Continue to answer questions and complete certification.

   ___ This is an existing information system with changes that create new privacy risks.

   Complete chart below, continue to answer questions, and complete certification.

<table>
<thead>
<tr>
<th>Changes That Create New Privacy Risks (CTCNPR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Conversions</td>
</tr>
</tbody>
</table>

2
<table>
<thead>
<tr>
<th>b. Anonymous to Non-Anonymous</th>
<th>e. New Public Access</th>
<th>h. Internal Flow or Collection</th>
</tr>
</thead>
<tbody>
<tr>
<td>c. Significant System Management Changes</td>
<td>f. Commercial Sources</td>
<td>i. Alteration in Character of Data</td>
</tr>
</tbody>
</table>

j. Other changes that create new privacy risks (specify):

---

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. Continue to answer questions and complete certification.

X 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 01-2015 or later). Skip questions and complete certification.

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. Please describe the activities which may raise privacy concerns.

---

No

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" (§11 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 for 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.)."

---

Yes, the IT system collects, maintains, or disseminates BII about: (Check all that apply.)

---

Companies

---

Other business entities (entities that obtain NIST-issued grants)

---

No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."
Yes, the IT system collects, maintains, or disseminates PII about: (Check all that apply.)

DOC employees
Contractors working on behalf of DOC
Members of the public

No, this IT system does not collect any PII.

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

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

Yes, the IT system collects, maintains, or disseminates PII other than user ID.

No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. 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.

Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

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, and/or 4c 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.
CERTIFICATION

X I certify the criteria implied by one or more of the questions above apply to the Grants Management Information System (142-01) 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 Grants Management Information System (142-01) and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO):
Jannet Cancino
Signature of SO: JANNET CANCEINO
Date: 2019.08.29 12:54:10 -04'00'

Name of Information Technology Security Officer (ITSO):
K. Robert Glenn
Signature of ITSO: KENNETH GLENN
Date: 2019.08.29 09:08:14 -04'00'

Name of Co-Authorizing Official (AO):
George Jenkins, Acting
Signature of AO: GEORGE JENKINS
Date: 2019.08.29 13:20:48 -04'00'

Name of Co-Authorizing Official (AO)/Bureau Chief Privacy Officer (BCPO):
Susannah Schiller, Acting
Signature of AO/BCPO: SUSANNAH SCHILLER
Date: 2019.08.07 15:46:10 -04'00'