

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



**Privacy Impact Assessment
for the
142-01 Grants Management Information System (GMIS)**

Reviewed by: Claire Barrett, 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

Jennifer Goode

09/30/2021

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: 142-01

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*

GMIS is used as the means of awarding and administering all issued grants and cooperative agreements administered by the NIST Grants Management Division (GMD).

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

GMIS is used as the means of awarding and administering all issued grants and cooperative agreements administered by the NIST Grants Management Division (GMD).

e. How information in the system is retrieved by the user

NIST internal users access the Commerce Business System (CBS) Portal logon page at <https://portal.cbs.nist.gov> and log into the CBS Portal application. 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 other DOC bureaus and offices (such as OS, NTIA and OIG) is via the DoC TLS network to the Herrbert C. Hoover Building (HCHB) in Washington, D.C. Other DOC 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.

f. 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 /GM IS F5 Local Traffic Manager (LTM).

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.

g. Any information sharing conducted by the system

Data is shared as follows:

- 1. DOC agencies to which NIST provides grant management/reporting support, which includes: NIST, Office of Inspector General (OIG), National Telecommunications & Information Administration (NTIA) and DOC Office of the Secretary**
- 2. General Service Administration System of Award Management (SAM) and Department of the Treasury Automated Standard Application for Payments (ASAP) for grantee information (via NIST 162-01 CBS/CFS).**
- 3. NIST 162-01, Commerce Business System/ Core Financial System (CBS/CFS)**
- 4. Health and Human Services Grants.gov**
- 5. DOC DataByDesign Grants Notification System (DBD GNS)**
- 6. Other internal NIST business units**

Data is shared with the DOC Office of Inspector General and other Government entities on a case-by-case basis for purposes of fraud, audit, or law enforcement.

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.;

5 U.S.C. 5701-5709 and 5721-5739, 28U.S.C.3101-3105, Debt Collection Act of 1982 (Pub. L. 97-365); 26 U.S.C. 6402(d); and 31 U.S.C. 3711. the Federal Information Security Management Act of 2002 (FISMA).

*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)
Taxpayer ID
Employer ID
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
Other general personal data:

Work-Related Data (WRD)
Job Title
Work Address
Work Telephone Number
Work Email Address
Salary
Other work-related data:

Distinguishing Features/Biometrics (DFB)
Other distinguishing features/biometrics:

System Administration/Audit Data (SAAD)
User ID
IP Address

Date/Time of Access
Other system administration/audit data:

Other Information

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

Directly from Individual about Whom the Information Pertains
Other:

Government Sources
Other Federal Agencies
Other:

Non-government Sources
Other:

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

The GMIS accepts data from Government systems and supplements this data for grants and cooperative agreements for services, goods, or materials provided by the vendor community to the Federal Government. Data is reviewed by the NIST GMD, NIST Financial Division, and grant program managers for accuracy and completeness.

2.4 Is the information covered by the Paperwork Reduction Act?

No, the information is not covered by the Paperwork Reduction Act.
The OMB control number and the agency number for the collection:

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?

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.

Purpose
For administrative matters
Other:

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).

The GMIS accepts data from Government systems and supplements this data for grants and cooperative agreements for services, goods, or materials provided by the vendor community to the Federal Government.

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.)

Unauthorized access could result in a breach of information. Information system security controls used to protect this information are implemented, validated, and continuously monitored. User access is restricted to authorized users and risk is minimized by limiting the number of authorized users. In addition, NIST requires and has in place:

- **Mandatory annual IT Security Training requirements**
- **Annual renewal of IT Security Rules of Behavior for NIST staff**
- **Policies and procedures for storage and disposal of sensitive electronic data**
- **System data encryption at rest and in transit**

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 - Federal Agencies 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:
<ul style="list-style-type: none"> • General Services Administration System for Award Management (SAM): via SFTP/SSH and stored on secure servers within the NIST protected network. • Department of the Treasury Automated Standard Application for Payments (ASAP): transmission of data to this application is a via point-to-point Virtual Private Network (VPN) over the Internet. • Health and Human Services Grants.gov via TLS encrypted web services. • DOC DataByDesign Grants Notification System (DBD GNS): via email (no sensitive data is sent to this application). • NIST 162-01 Commerce Business System/ Core Financial System (CBS/CFS): data is transmitted over internal NIST network in firewall protected zones. Data on the CBS/CFS is encrypted at rest and in transit.

- 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.

Yes, notice is provided by other means.
The Privacy Act statement and/or privacy policy can be found at:
The reason why notice is/is not provided:
Grantees are notified if their PII/BII is collected, maintained, or disseminated through the GSA SAM and ASAP registration processes.

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

No, individuals do not have an opportunity to decline to provide PII/BII in GMIS.
The reason why individuals can/cannot decline to provide PII/BII:
Grantees have opportunity to decline providing PII/BII with GSA SAM and ASAP. However, doing so may result in not doing business with the Federal Government.

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 in GMIS.
The reason why individuals can/cannot consent to particular uses of their PII/BII:
Grantees have opportunity to consent to particular uses of their PII/BII when registering with GSA SAM or ASAP.

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 in GMIS.
The reason why individuals can/cannot review/update PII/BII:
Grantees may review and update their profiles within GSA SAM, or records within ASAP.

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system.

All users are subject to a Code of Conduct that includes the requirement for confidentiality.
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.
Reason why access to the PII/BII is being monitored, tracked, or recorded:
Access logs are kept and reviewed for anomalies.

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). 09/30/2020
Other administrative and technological controls for the system:

- 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).*

<p>The application is accessible on internal NIST networks protected by multiple layers of firewalls. Unauthorized use of the system is restricted by user authentication. Access logs are kept and reviewed for anomalies on an as needed basis. Data is stored on servers located at the NIST Gaithersburg, Maryland facility within the continental United States. Data on the servers is encrypted at rest and in motion.</p> <p>For information sharing, PII is transferred in a secure fashion. To guard against the interception of communication over the network, the components use the Transport Layer Security (TLS) protocol which encrypts communications, or FIPS 140-2 encrypted virtual private network technologies between organizations. Access to GMIS requires NIST-issued credentials because access is restricted by user authentication. Other agency users access GMIS from an authorized DOC network or by connecting to the NIST network through a Virtual Private Network (VPN).</p>

Section 9: Privacy Act

- 9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?
No, 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:
GRS 1.2/020 Successful applications
The stage in which the project is in developing and submitting a records control schedule:

No, retention is not monitored for compliance to the schedule.
Reason why retention is not monitored for compliance to the schedule:
The GMIS does not have the technical capability to archive/purge records.

10.2 Indicate the disposal method of the PII/BII.

Disposal
Shredding
Degaussing
Other (specify)
Other disposal method of the PII/BII:
The GMIS does not have the technical capability to archive/purge records.

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
Quantity of PII Context of Use Obligation to Protect Confidentiality	<p>Quantity of PII-A Taxpayer Identification Number (TIN) is an identification number used by the Internal Revenue Service (IRS) in the administration of tax laws. It is issued either by the Social Security Administration (SSA) or by the IRS. A Social Security number (SSN) is issued by the SSA whereas all other TINs are issued by the IRS.</p> <p>Context of Use-The purpose for which the information is collected supports the administrative business of NIST.</p> <p>Obligation to Protect Confidentiality-Potential for proprietary business processes to be included in grant submission packages.</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.)

Unauthorized access could result in a breach of information. Information system Security controls used to protect this information are implemented, validated, and continuously monitored. User access is restricted to authorized users, and risk is minimized through limiting the number of authorized users.

Mitigating controls:

GMIS implements a data retention schedule and disposal plan. Only data required for the GMIS mission is used in GMIS. All GMIS users are subject annual training requirements and rules of behavior which can raise the necessary awareness to mitigate data mishandling.

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