United States Environmental Protection Agency

# PRIVACY IMPACT ASSESSMENT

*(Rev. 2/2020)*
*(All Previous Editions Obsolete)*

Please submit your responses to your Liaison Privacy Official.
***All entries must be Times New Roman, 12pt, and start on the next line.***
If you need further assistance, contact your LPO. A listing of the LPOs can be found here:
https://usepa.sharepoint.com/:w:/r/sites/oei_Community/OISP/Privacy/LPODoc/LPO%20Roster.docx

| | |
|---|---|
| **System Name:**<br><br>Next Generation Grants System (NGGS) | |
| **Preparer:**<br><br>Carlyn Perry | **Office:**<br><br>OMS/OGD |
| **Date:**<br><br>03/26/2020 | **Phone:**<br><br>202 564-5309 |
| **Reason for Submittal: New PIA_ __ Revised PIA__X__ Annual Review____ Rescindment ____** | |
| **This system is in the following life cycle stage(s):** | |
| Definition ☐ Development/Acquisition ☒ Implementation ☐ | |
| Operation & Maintenance ☐ Rescindment/Decommissioned ☐<br><br>**Note: New and Existing Systems require a PIA annually, when there is a significant modification to the system or where privacy risk has increased to the system. For examples of significant modifications, see OMB Circular A-130, Appendix 1, Section (c) (1) (a-f).**<br><br>**The PIA must describe the risk associated with that action. For assistance in applying privacy risk see OMB Circular No. A-123, Section VII (A) (pgs. 44-45).** | |

## Provide a general description/overview and purpose of the system:

The Next Generation Grants System (NGGS) processes the Agency Grants and Interagency Agreements. The Next Generation Grants System (NGGS) contains information on the recipient of the grant, fellowship, cooperative agreement and interagency agreement, including the name of the entity accepting the award. This is usually an organization, with the exception of fellowships, which are awarded to persons, and interagency agreements which are awarded to other federal agencies. This is a modification to the existing

IGMS PIA to reflect the change to NGGS and the platform is being modernized from Lotus Notes to an Oracle/Java platform.

# Section 1.0 Authorities and Other Requirements

## 1.1 What specific legal authorities and/or Executive Order(s) permit and define the collection of information by the system in question?

Federal Grant and Cooperative Agreement Act, 31 U.S.C. 6301 *et seq.*; Clean Air Act, 42 U.S.C. 1857 *et seq.*; Federal Water Pollution Control Act, 33 U.S.C. 1254 *et seq.*; Public Health Service Act, 42 U.S.C. 241 *et seq.*; Solid Waste Disposal Act, 42 U.S.C. 6901 *et seq.*; Federal Insecticide, Fungicide, and Rodenticide Act, 7 U.S.C. 136 *et seq.*; Safe Drinking Water Act, 42 U.S.C. 300j-1; Toxic Substances Control Act, 15 U.S.C. 2609, Comprehensive Environmental Response, Compensation, and Liability Act, 42 U.S.C. 9660.

## 1.2 Has a system security plan been completed for the information system(s) supporting the system? Does the system have or will the system be issued an Authorization-to-Operate? When does the ATO expire?

Yes, a SSP been completed for NGGS. Yes, NGGS will be issued an ATO.

## 1.3 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Yes. OMB 4040-0004; 4040-0006;

## 1.4 Will the data be maintained or stored in a Cloud? If so, is the Cloud Service Provider (CSP) FedRamp approved? What type of service (PaaS, IaaS, SaaS, etc.) will the CSP provide?

No.

# Section 2.0 Characterization of the Information

*The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.*

## 2.1 Identify the information the system collects, uses, disseminates, or maintains (e.g., data elements, including name, address, DOB, SSN).

Information collected includes recipient name, recipient mailing address, recipient phone number, recipient email address, recipient program manager first name, recipient program manager last name, Dun and Bradstreet Number and tax identification number.

### 2.2 What are the sources of the information and how is the information collected for the system?

Information about recipients applying for Grants and Interagency Agreements. The information is collected electronically from the recipient from Grants.GOV via OMS EI Central Data Exchange (CDX). User Accounts for EPA employees is pulled from the Agency Directory Services.

### 2.3 Does the system use information from commercial sources or publicly available data? If so, explain why and how this information is used.

Yes. We use Grants.Gov and the System for Award Management (SAM.GOV). The information collected supports the purpose of the Office of Grants Debarment Grants Program. The EPA Grants Office collects information that is directly relevant and necessary to accomplish the awarding of grants.

### 2.4 Discuss how accuracy of the data is ensured.

Data from recipients is assumed to be accurate. EPA Grants Specialist and Project Officer verify the accuracy of the data using the System for Award Management (SAM.GOV) the authoritative source for the recipient. The recipient updates their data in System for Award Management (SAM.GOV) when a change occurs in the recipient status/information change due address, DUNS etc.

### 2.5 Privacy Impact Analysis: Related to Characterization of the Information

*Discuss the privacy risks identified for the specific data elements and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.*

**Privacy Risk:**

Risk EPA staff inadvertently distribute data in the NGGS system due to human error.

**Mitigation:**

There are appropriate controls in place. ROB is also signed by EPA staff to prevent unauthorised information distribution. Mandatory annual Information Security and Privacy Awareness Training is completed by all Agency staff and contractors.

## Section 3.0 Access and Data Retention by the System

*The following questions are intended to outline the access controls for the system and how long the system retains the information after the initial collection.*

### 3.1 Do the systems have access control levels within the system to prevent authorized users from accessing information they don't have a need to

**know? If so, what control levels have been put in place? If no controls are in place why have they been omitted?**

Yes, each user in NGGS is designated a user role within the system based on their access and assigned role.

NGGS is managed by the system administrator in the Office of Grants and Debarment who assigns roles and responsibilities within the system to users in who are responsible for Grants Management. User roles and responsibilities for the Grants Management is determined by the staff's manager within their organization. User access is based on the roles users are assigned in the system.

## 3.2 In what policy/procedure are the access controls identified in 3.1, documented?

The Access Control List is documented in the SSP.

NGGS is managed by the system administrator in the Office of Grants and Debarment who assigns roles and responsibilities within the system to users in who are responsible for Grants Management. User roles and responsibilities for the Grants Management is determined by the staff's manager within their organization.

## 3.3 Are there other components with assigned roles and responsibilities within the system?

Assigned roles and responsibilities within NGGS are provided only to registered NGGS EPA personnel. There are no other components within NGGS with assigned roles and responsibilities

## 3.4 Who (internal and external parties) will have access to the data/information in the system? If contractors, are the appropriate Federal Acquisition Regulation (FAR) clauses included in the contract?

Science Application International Corporation (SAIC) contractors have an Agency level contract. Yes, we have applied the GS Schedule and FAR clauses to the contract.

## 3.5 Explain how long and for what reasons the information is retained. Does the system have an EPA Records Control Schedule? If so, provide the schedule number.

Records are retained in accordance with EPA's Record Schedule 009 and disposed of under National Archives and Records Administration (NARA) disposal authority NARA Disposal Authority: N1-412-07-33c.

Item c: Electronic data - Superfund site-specific
This item is to be used only by the Office of Administration and Resources Management, Grants Management Division at Headquarters. NARA Disposal Authority: N1-412-07-33c; Disposable; Destroy 30 years after grant closeout.
Item d: Electronic data - waste water construction and state revolving fund grants

This item is to be used only by the Office of Administration and Resources Management, Grants Management Division at Headquarters.
NARA Disposal Authority: N1-412-07-33d; Disposable
Destroy 20 years after grant closeout.
Item e: Electronic data - other than Superfund site-specific, waste water construction, and state revolving fund grants
This item is to be used only by the Office of Administration and Resources Management, Grants Management Division at Headquarters. NARA Disposal Authority: NARA Disposal Authority: N1-412-07-33e; Disposable; Destroy 10 years after grant closeout.

### 3.6 Privacy Impact Analysis: Related to Retention

*Discuss the risks associated with the length of time data is retained. How were those risks mitigated? The schedule should align the stated purpose and mission of the system.*

**Privacy Risk:**

Information may be retained longer than needed.

**Mitigation:**

The records retention schedule applicable to NGGS is properly followed.

## Section 4.0 Information Sharing

*The following questions are intended to describe the scope of the system information sharing external to the Agency. External sharing encompasses sharing with other federal, state and local government, and third-party private sector entities.*

### 4.1 Is information shared outside of EPA as part of the normal agency operations? If so, identify the organization(s), how the information is accessed and how it is to be used, and any agreements that apply.

No

### 4.2 Describe how the external sharing is compatible with the original purposes of the collection.

N/A

### 4.3 How does the system review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within EPA and outside?

N/A

### 4.4 Does the agreement place limitations on re-dissemination?

N/A

### 4.5 Privacy Impact Analysis: Related to Information Sharing

*Discuss the privacy risks associated with the sharing of information outside of the agency. How were those risks mitigated?*

**Privacy Risk:**

None. There is no external sharing

**Mitigation:**

None.

# Section 5.0 Auditing and Accountability

*The following questions are intended to describe technical and policy-based safeguards and security measures.*

## 5.1 How does the system ensure that the information is used as stated in Section 6.1?

NGGS maintains an audit trail documenting the actions that users take in the system. NGGS is limited to registered EPA employees with assigned roles and responsibilities. Each user has access that is limited to the user role based on their role in the Access Control List.

## 5.2 Describe what privacy training is provided to users either generally or specifically relevant to the system/collection.

The Information Security and Privacy Awareness Training is mandatory each year. The course includes information regarding policies and practices that EPA users should follow. The Privacy Act of 1974 and Rules of Behaviors are also discussed.

## 5.3 Privacy Impact Analysis: Related to Auditing and Accountability

**Privacy Risk:**

There is a low risk of unauthorized access to the system. If a system does not have technical controls and policy based on safeguarding security measure that can be audited. Not ensuring users are being held accountable for compliance with policy regarding access to a system may present a risk.

**Mitigation:**

Auditing and accountability checks are done on a daily basis to ensure safeguarding of NGGS data. NGGS includes access controls and audit trail for grant information. Users of the system must take the Agency Mandatory Information Security and Privacy Awareness Training and NGGS Rules of Behavior training yearly to maintain access to the system.

# Section 6.0 Uses of the Information

*The following questions require a clear description of the system's use of information.*

## 6.1 Describe how and why the system uses the information.

The EPA Office of Grants and Debarment uses information in the NGGS to Award Grants to the Recipient. Use of the recipient mailing address and e-mail address information in NGGS is used to provide notification to recipients. This information is used to verify and validate information of recipients applying for Grants and Interagency Agreements.

## 6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes_X_ No___. If yes, what identifier(s) will be used.

*(A personal identifier is a name, social security number or other identifying symbol assigned to an individual, i.e. any identifier unique to an individual. Or any identifier that can be linked or is linkable to an individual.*)

All grants in NGGS are assigned a grant number and identified by the grant number and applicant name. Information may be retrieved by using the applicant name and/or the grant number.

## 6.3 What type of evaluation has been conducted on the probable or potential effect of the privacy of individuals whose information is maintained in the system of records?

Security controls used to protect personal sensitive data in Next Generation Grants System (NGGS) are commensurate with those required for an information system rated moderate for confidentiality, integrity, and availability, as prescribed in NIST Special Publication, 800-53, "Recommended Security Controls for Federal Information Systems," Revision 4.

Administrative Safeguards

- Paper records are maintained in locked file cabinets.

Technical Safeguards

- Electronic records are maintained in a secure, password protected electronic system.

Physical Safeguards

- All records are maintained in secure, access-controlled areas or buildings.

## 6.4 Privacy Impact Analysis: Related to the Uses of Information

*Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.*

**Privacy Risk:**

There is a risk that information collected and contained in NGGS could be misused.

**Mitigation:**

To mitigate any privacy risks with regards to use of information in NGGS. Access to NGGS is limited to registered EPA users who have completed the Rules and Behavior, Project Officer and Grants training related to the user role and responsibility. Access is given after all training has been completed.

*If no SORN is required, STOP HERE.

*The NPP will determine if a SORN is required. If so, additional sections will be required.*

## Section 7.0 Notice

*The following questions seek information about the system's notice to the individual about the information collected, the right to consent to uses of information, and the right to decline to provide information.*

### 7.1 How does the system provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Any individual who wants to know whether this system of records contains a record about him or her, should make a written request to the Attn: Agency Privacy Officer, MC 2831T, 1200 Pennsylvania Ave., NW., Washington, D.C. 20460, privacy@epa.gov.

### 7.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the collection or sharing of their information?

NGGS collects grants applicant information through federal-wide H.H.S. Grants.gov portal. Since applicants apply for grants directly in Grants.gov, NGGS relies on the workflow process in Grants.gov to collect consent from the applicant.

### 7.3 Privacy Impact Analysis: Related to Notice

*Discuss how the notice provided corresponds to the purpose of the project and the stated uses. Discuss how the notice given for the initial collection is consistent with the stated use(s) of the information. Describe how the project has mitigated the risks associated with potentially insufficient notice and opportunity to decline or consent.*

**Privacy Risk:**

The privacy risk related to notice is associated with potentially insufficient notice of privacy data collection prior to the agency providing actual or constructive notice of a grant award.

**Mitigation:**

Notice is provided to the individual in this PIA and SORN EPA-53 regarding the collection and use of privacy information. The information is used only for the purpose for which the notice was provided

## Section 8.0 Redress

*The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.*

### 8.1 What are the procedures that allow individuals to access their information?

Individuals seeking access to information in this system of records about themselves are required to provide adequate identification (e.g., driver's license, military identification card, employee badge or identification card). Additional identity verification procedures may be required, as warranted. Requests must meet the requirements of EPA regulations that implement the Privacy Act of 1974, at 40 CFR part 16.

## 8.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Requests for correction or amendment must identify the record to be changed and the corrective action sought. Complete EPA Privacy Act procedures are described in EPA's Privacy Act regulations at 40 CFR part 16 and referenced in SORN EPA-53.

## 8.3 Privacy Impact Analysis: Related to Redress

*Discuss what, if any, redress program the project provides beyond the access and correction afforded under the Privacy Act and FOIA.*

**Privacy Risk:**

None. There is an appropriate procedure in place related to redress.

**Mitigation:**

None.