



U.S. Department of the Interior PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the [DOI PIA Guide](#) for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project: GrantSolutions HHS Cloud Offering

Bureau/Office: Office of the Secretary (OS)

Date: September 20, 2022

Point of Contact:

Name: Danna Mingo

Title: OS Departmental Offices Associate Privacy Officer

Email: Danna_Mingo@ios.doi.gov

Phone: 202-441-5504

Address: 1849 C Street NW, Mail Stop 7112 MIB, Washington, DC 20240

Section 1. General System Information

A. Is a full PIA required?

- Yes, information is collected from or maintained on
- Members of the general public
 - Federal personnel and/or Federal contractors
 - Volunteers
 - All
- No:

B. What is the purpose of the system?

GrantSolutions is a financial assistance management software platform used for managing grants and cooperative agreements through the award lifecycle. This web-based, grant management platform is offered as a shared service by the Department of Health and Human Services (HHS) to multiple federal agencies, to allow agencies to manage Federal financial assistance (also referred to as grants or cooperative agreements)



issued across the Department. The Department of the Interior (DOI) has entered into such an agreement with HHS, allowing DOI access to GrantSolutions to effectively administer the grants issued by DOI's Bureaus and offices.

GrantSolutions supports the application, review, approval, and award of assistance grants in a decentralized environment. The core business processes of the system involve:

- Discretionary/Formula/Block Grant Application Processing awards and grantee information;
 - Grant Application merit review and eligibility screening;
 - Funds Control - grant commitments and non-grant expenditures; and
 - Grant Oversight - post-award reporting, and maintenance of grant information
- Grantees and Applicants may be internal or external, Federal or non-Federal employees. Grant Awarding Officers must be Federal employees.

DOI grant agreements are initiated by bureau and office employees who log into GrantSolutions via a web-based interface and create a "federal opportunity announcement." DOI grant offices enter data into GrantSolutions to describe the purpose of the grant, who may apply for the grant, and how to apply for a grant. Once the grant information is entered into GrantSolutions, the system creates a publicly viewable announcement, which is transmitted and posted to grants.gov. Grants.gov is another HHS-owned system that serves as the central location for all federal government grant announcements. Once a grant announcement is posted to grants.gov, non-federal entities or individuals can review the announcement and determine if they wish to apply for a federal grant. Business entities completing the grant or cooperative agreement process may utilize the System for Award Management (Sam.gov), a GSA-owned, government-wide portal which assists grant officials with pre-award determinations and management of federal awards throughout the awards life-cycle.

Non-federal entities or individuals who wish to apply for a DOI grant will view the announcement on grants.gov and apply for the grant directly in grants.gov. The announcement will contain the instructions for how to apply, what forms need to be submitted, any applicable deadlines, and any other applicable restrictions. Applicants will access the required forms directly in grants.gov and in most cases, will submit their entire application directly in grants.gov.

Upon the closing date of the announcement, the applications that were submitted in grants.gov are pulled back into GrantSolutions, where the associated DOI grant office can then log back into GrantSolutions, review the applications within GrantSolutions, and make a determination of which entities will receive a grant and how much grant funding to provide to an applicant. The application review steps are done directly within GrantSolutions, and GrantSolutions maintains a record of this application review process.



Once a determination is made to provide grant funding to an applicant, DOI program offices then begin the process of certifying government funds for a grant using the DOI Financial and Business Management (FBMS) system, which will document when the grant has been awarded, as well as distribute the grant funding. The application number serves as the link between FBMS and GrantSolutions to identify the availability of funds for a specific application.

As funds are certified, the DOI Grant Office will then log back into GrantSolutions to create the final grant agreement between the DOI and the applicant. GrantSolutions will automatically pull data elements from the application documents to create a final grant agreement. Once the grant office is ready to proceed with the final agreement, GrantSolutions will also use the application data to conduct a variety of application eligibility checks. This includes a check of external federal systems to validate the applicant is eligible to receive government funds (i.e. applicant is not disbarred from doing business with the government, applicant is not on a federal “do not pay list,” applicant does not have negative audit findings that need to be resolved, etc.) If the applicant passes all the application eligibility checks, GrantSolutions will identify the application to the DOI grant office as being eligible to receive a grant. The DOI grant office will then “release” the grant in GrantSolutions. When a grant is released in GrantSolutions, the final resulting grant agreement is made available to the applicant directly in GrantSolutions.

Twice a month, GrantSolutions provides a report of all DOI grant awards to USASpending.gov in accordance with the Digital Accountability and Transparency (DATA) Act, which requires federal agencies to report their spending information.

The information collected within GrantSolutions during the application process, award agreement process, and any other data that is collected post award remains housed within the GrantSolutions database, owned and operated by HHS.

C. What is the legal authority?

Federal Funding Accountability and Transparency Act, DATA Act and 2 CFR 200, Grants and Agreements

D. Why is this PIA being completed or modified?

- New Information System
- New Electronic Collection
- Existing Information System under Periodic Review
- Merging of Systems
- Significantly Modified Information System
- Conversion from Paper to Electronic Records



- Retiring or Decommissioning a System
- Other

E. Is this information system registered in CSAM?

- Yes:

CSAM ID 2606 – GrantSolutions HHS System Security and Privacy Plan
UII Code: 010-000002735

- No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

| Subsystem Name | Purpose | Contains PII (Yes/No) | Describe <i>If Yes, provide a description.</i> |
|----------------|---------|--------------------------|---|
| None | None | No | N/A |

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

- Yes:

INTERIOR/DOI-89, Grants and Cooperative Agreements: FBMS - 73 FR 43775 (July 28, 2008); modification published 86 FR 50156 (September 7, 2021)

- No

H. Does this information system or electronic collection require an OMB Control Number?

- Yes:

The Department of the Interior (DOI) does not own the forms that collect the personally identifiable information (PII) for GrantSolutions. The forms are owned and managed by HHS. The specific forms an applicant completes are determined on a program-by-program basis by the Awarding Office staff and is identified in the announcement. All forms must be approved by the Office of Management and Budget (OMB), with a Privacy Act Statement, and grants.gov maintains the menu of forms that can be selected



on the family forms website: <https://www.grants.gov/forms/sf-424-family.html>. This website contains the OMB Control Number and expiration date for the forms.

No

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.

- Name
- Personal Cell Telephone Number
- Personal Email Address
- Home Telephone Number
- Mailing/Home Address
- Other:

Non-federal employees and members of the public who submit grant applications may use a Taxpayer Identification Number (TIN), and a company submitting a grant application may use an Employer Identification Number (EIN). SSN may be provided by applicants, although not solicited as part of the grant application process. When detected, SSN is removed by grant administrators.

B. What is the source for the PII collected? Indicate all that apply.

- Individual
- Federal agency
- Tribal agency
- Local agency
- DOI records
- Third party source
- State agency
- Other:

GrantSolutions interfaces with Grants.gov and Sam.gov, as part of the grant application process and for pre-award determinations. Sam.gov is a GSA-owned, government-wide portal which assists grant officials with pre-award determinations and management of federal awards throughout the awards life-cycle. Applicants will also use grants.gov as part of the application process, to include: forms that provide additional information on how the applicant intends to spend grant funds, schedules, diagrams, pictures, etc.



C. How will the information be collected? Indicate all that apply.

- Paper Format
- Email
- Face-to-Face Contact
- Web site
- Fax
- Telephone Interview
- Information Shared Between Systems
- Other:

Most applications are submitted through Grants.gov. However, individuals or businesses may download and submit applications through email, mail or fax. Individuals or businesses may also submit applications directly into GrantSolutions. Applications submitted through mail, email, or fax are manually entered into GrantSolutions by authorized personnel at respective Bureaus and Offices.

D. What is the intended use of the PII collected?

The primary use of the PII collected is to maintain grant recipient vendor information associated with grants and cooperative agreement awards. It may also be used by Awarding Offices to evaluate applicant risks and validate grant recipient eligibility through searches of databases, such as the federal audit clearing house, and validate grant eligibility to determine any negative information prior to awarding the grant.

E. With whom will the PII be shared, both within DOI and outside DOI? Indicate all that apply.

- Within the Bureau/Office:

The Office of Financial Management (PFM), Office of Grants Management (PGM), and the Business Integration Office (BIO) have access to GrantSolutions, and can view information for all bureaus within DOI. They are responsible for the management and oversight of the grants and cooperative agreement awards within DOI, including creating and implementing policy and procedures for these awards.

- Other Bureaus/Offices:

The information within GrantSolutions may be accessible to other bureaus/offices within DOI for the primary purpose of awarding and managing grant and cooperative agreement awards. Access to information in GrantSolutions is controlled through role and office assignments. Each Bureau's office has access to their own data associated with the grant



agreements issued out of their office. Access may be expanded for awarding offices on an as-needed basis to assist with workload sharing or cross-bureau/office actions.

Other Federal Agencies:

Information is shared with other Federal agencies (HHS) in accordance with the disclosures detailed in INTERIOR/DOI-89, Grants and Cooperative Agreements: FBMS - 73 FR 43775 (July 28, 2008); modification published 86 FR 50156 (September 7, 2021) SORN, which can be reviewed at the following url: <https://www.doi.gov/privacy/doi-89-grants-and-cooperative-agreements-fbms>.

In accordance with the Federal Funding Accountability and Transparency Act (FFATA) and the DATA Act, key information pertaining to Federal awards is transmitted from GrantSolutions into USASpending.gov. The data elements provided are defined by the DATA Act Information Model schema maintained by the Department of Treasury. No PII is shared as part of this report. Information pertaining to the USASpending.gov reporting elements can be located on the Department of Treasury's Data Transparency Program webpage: <https://fiscal.treasury.gov/data-transparency/>.

Tribal, State or Local Agencies:

Information may be shared with Tribal, State, or Local Agencies in accordance with the disclosures detailed in INTERIOR/DOI-89, Grants and Cooperative Agreements: FBMS - 73 FR 43775 (July 28, 2008); modification published 86 FR 50156 (September 7, 2021) SORN, which can be reviewed at the following url: <https://www.doi.gov/privacy/doi-89-grants-and-cooperative-agreements-fbms>.

Contractor:

Information is shared with Bureaus/offices contractors that support the grants management program and other routine uses in accordance with the disclosures detailed in INTERIOR/DOI-89, Grants and Cooperative Agreements: FBMS - 73 FR 43775 (July 28, 2008); modification published 86 FR 50156 (September 7, 2021) SORN, which can be reviewed at the following url: <https://www.doi.gov/privacy/doi-89-grants-and-cooperative-agreements-fbms>.

Other Third-Party Sources:

Information is shared with other third-party sources such as organizations and entities which is limited to their own information in accordance with the disclosures detailed in INTERIOR/DOI-89, Grants and Cooperative Agreements: FBMS - 73 FR 43775 (July 28, 2008); modification published 86 FR 50156 (September 7, 2021) SORN, which can be reviewed at the following url: <https://www.doi.gov/privacy/doi-89-grants-and-cooperative-agreements-fbms>.



F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

Yes:

Individuals voluntarily provide the information in the application, but declining to provide this information may affect the processing of the grant application.

No:

G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

Privacy Act Statement:

All forms must be OMB approved with a Privacy Act Statement. The HHS forms are maintained on Grants.gov, and the required forms may be selected on the FS-424 Family page: <https://www.grants.gov/forms/sf-424-family.html>.

Privacy Notice:

Notice is provided through publication of this PIA and the INTERIOR/DOI-89, Grants and Cooperative Agreements: FBMS - 73 FR 43775 (July 28, 2008); modification published 86 FR 50156 (September 7, 2021) SORN which can be reviewed at the following url: <https://www.doi.gov/privacy/doi-89-grants-and-cooperative-agreements-fbms>.

Other: Privacy notice is listed on grantsolutions.gov and hhs.gov

None

H. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).

Personal identifiers may be used to retrieve data in GrantSolutions, to include: applicant name, TIN, Unique Entity Identifier (UEI) Assigned at Award).

I. Will reports be produced on individuals?

Yes:

Reports are pulled twice a month per the DATA Act and uploaded on the USASpending.gov website, in accordance with the Federal Funding Accountability and



Transparency Act (FFATA) and the DATA Act. The report includes the grantee name, address, and the award information. The information is sent to USASpending.gov and the DOI bureaus and offices. The data elements provided are defined by the DATA Act Information Model schema maintained by the Department of Treasury. Information pertaining to the USASpending.gov reporting elements can be located on the Department of Treasury's Data Transparency Program webpage: <https://fiscal.treasury.gov/data-transparency/>.

No

Section 3. Attributes of System Data

A. How will data collected from sources other than DOI records be verified for accuracy?

Data is collected directly through applicants submitting grant applications via Grants.gov and Sam.gov. Non-Competitive Grants can be submitted directly into GrantSolutions. However, the system performs validation and reconciliation of information at each system-to-system interface to ensure that the data is transferred and stored properly, without data errors.

B. How will data be checked for completeness?

Data will be checked for completeness as it is entered into the system. DOI and GrantSolutions has built quality checks into the system to determine if that data is complete or valid. One type of verification of completeness check involves a system-to-system check against the vendor data stored within SAM.gov. If the data is not successfully validated, the system will display an error.

C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

Data is checked to see if it is current and not duplicated by comparing the incoming data with the data in the system. The check is performed when being processed through GrantSolutions. Sam.gov requires entities to update and renew their registration yearly. Contractors are also required to maintain their registration and ensure it is current.

Most of the data collected from sources other than DOI and GrantSolutions comes from Sam.gov and Grants.gov, and is deemed to be current. In all cases, data is automatically checked for accuracy by comparing the incoming data with the data already in the system as the data is processed.



D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.

GrantSolutions retains grant records for 20 years after the final action for use in Artificial Intelligence and Machine Learning to increase the efficiency of the Grants Management Lifecycle and improve outcomes for the American public. The research business case is approved by HHS. While all agency partners have final ownership of their grants data, DOI may request final disposition for individual grant records after 10 years per GRS 1.2 for any record they do not wish to be processed per the GS-SF115 disposition schedule. For any grant record that an agency Partner deems historically significant and must be permanent – the Partner has the responsibility to maintain the permanent record outside of GrantSolutions. In accordance with GRS 1.2, GrantSolutions is a temporary system for temporary grant records and retains a copy of the permanent record for use in grant administration.

E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?

While all partners have final ownership of their grants data, DOI may request final disposition for individual grant records after 10 years per GRS 1.2 for any record they do not wish to be processed per the GS-SF115 disposition schedule.

For any grant record that a Partner deems historically significant and must be permanent – the Partner has the responsibility to maintain the permanent record outside of GrantSolutions. In accordance with GRS 1.2, GrantSolutions is a temporary system for temporary grant records and retains a copy of the permanent record for use in grant administration.

F. Briefly describe privacy risks and how information handling practices at each stage of the “information lifecycle” (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.

There is a risk to individual privacy due to the personal information collected and maintained in GrantSolutions. These risks are mitigated through administrative, physical and technical controls that have been implemented to protect the confidentiality, integrity and availability of the information. Security and privacy controls are implemented in accordance with the Privacy Act of 1974, Federal Information Security Modernization Act of 2014 (FISMA), OMB Circular A-130, *Managing Information as a Strategic Resource*, OMB Circular A-123, *Management’s Responsibility for Internal Control*, and



National Institute of Standards and Technology (NIST) SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*.

There is a risk that data may be inappropriately accessed or disclosed or used for unauthorized purposes. Access is restricted by each bureau and office. Bureaus and offices can only see grant information for their organization. PGM, PFM, and BIO has Department-wide access and can view all bureau and office Grants information. Access to GrantSolutions is based on the FBMS Governance Risk and Compliance (GRC) Role Based access. DOI users processing grants will need to be assigned a specific role to be able to access and process grants. All DOI employees and contractors are required to complete privacy, security and records management awareness training, as well as role-based on an annual basis, and sign the DOI Rules of Behavior prior to accessing any system.

There is a risk that data may be stored for longer than necessary. Records are maintained and disposed of under a NARA-approved records schedule. User accounts containing PII that are inactive are disabled by system administrators, however, user created content is maintained as long as it remains active or as deemed necessary by DOI. Information collected and stored within GrantSolutions is maintained, protected, and destroyed in compliance with all applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

Yes:

GrantSolutions is a grants management system used by DOI that provides automated support for Federal grant decision-making and accountability. GrantSolutions supports the application, review, approval, and award of assistance grants in a decentralized environment.

No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

Yes:

No



C. Will the new data be placed in the individual's record?

Yes:

No

D. Can the system make determinations about individuals that would not be possible without the new data?

Yes:

No

E. How will the new data be verified for relevance and accuracy?

Not applicable. GrantSolutions does not derive new data or create previously unavailable data about an individual through data aggregation.

F. Are the data or the processes being consolidated?

Yes, data is being consolidated.

Yes, processes are being consolidated.

No, data or processes are not being consolidated.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

Users: GrantSolutions users will have access to the system

Contractors: FBMS contractors supporting Grantsolutions

System Administrator

Other: PFM, PGM, and BIO officials have Department-wide access to data in GrantSolutions.

H. How is user access to data determined? Will users have access to all data or will access be restricted?

Registered applicants/recipients have access to the system, and they must request a UID/Password. Users submit requests to GrantSolution for approval and account access using login.gov. Users will be provided a UID/Password to login. Once a recipient/applicant receives GrantSolutions systems access, they will initially only have access to application data they have input into GrantSolutions. An individual within an



organization may also receive access to additional information pertaining to grants issued to their organization with approval from both their organization and the federal government awarding officer who issued their grant. Recipient access to grant specific data is controlled by the federal government financial assistance awarding officer who issued the agreement.

FBMS users accessing GrantSolutions will follow Governmental and Departmental standards for application access controls. All system access requires Security Assertion Markup Language (SAML) Personal Identity Verification (PIV) authentication to access the systems. The FBMS Access Control Policy and Grant Solutions DOI-GMM Account Creation Process SOP Version 1.1 outlines the requirements for gaining access to FBMS and GrantSolutions.

Bureau/Office administrators are responsible for controlling and monitoring access of authorized employees. Bureau/Office Administrators and authorized employees will only receive access to data for their own Bureau or Office. A user must have a valid DOI Active Directory (AD) account prior to submitting a new user registration request for GrantSolutions. The request is initiated in GRC and processed through automated approvals by the requisite parties (Bureau Security Points of Contact (SPOCs) and Bureau Account Controllers). The SPOC and Account Controller must approve the new user registration request before the user is granted access to GrantSolutions. Once established in the system, account privileges can be assigned to users as part of a role-based access control security model. Role requests are also initiated in GRC and processed through automated approvals involving Bureau Security Points of Contact (SPOCs), Bureau Account Controllers, Bureau Internal Controls Coordinators, and Bureau Training Coordinators.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

Yes

GrantSolutions is hosted by HHS in the Amazon Web Services (AWS) East Region. Maintenance of the system will be handled by HHS. DOI depends on HHS to ensure the appropriate Privacy clauses are maintained in the contract.

No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

Yes.

No



K. Will this system provide the capability to identify, locate and monitor individuals?

Yes.

GrantSolutions system logs can be used to run reports detailing an individual user's authorized access and actions performed within the system, to include attempts to access files or transactions beyond the user's assigned permissions. The logs capture account creation, modification, disabling, and termination in the logs. The application name, date and time, item ID, type, location, event type date, and action taken on item is captured in the logs. These logs are captured within the GrantSolution application and only authorized users have access to the logs. Syslogs are enabled on all host and server systems as well as the firewalls and other network perimeter security devices and IDS.

No

L. What kinds of information are collected as a function of the monitoring of individuals?

The system is not intended to monitor individuals; however, the system will have the ability to audit the usage activity in the system, including the use by system administrators, Departmental Manager, Bureau/Office Managers, and other resources. Audit information includes reviewable data such as login date and time. In addition, the system will monitor workflow, including monitoring the status of reviews of new and existing Grants.

M. What controls will be used to prevent unauthorized monitoring?

Controls outlined in the GrantSolutions HHS System Security and Privacy Plan that adhere to the standards outlined in NIST SP 800-53, *Recommended Security and Privacy Controls for Federal Information Systems*, are in place to prevent unauthorized monitoring. This includes the use of role-based security training, encryption, and maintaining data in secured facilities, among others. FBMS assigns roles based on the principles of least privilege and performs due diligence toward ensuring that separation of duties is in place.

Only DOI authorized users with valid DOI Active Directory and GrantSolutions credentials will be able to access the system. In addition, all users must consent to Rules of Behavior and complete Federal Information System Security Awareness, Privacy and Records Management training before being granted access to the DOI network or any DOI system, and annually thereafter.

FBMS-Cloud has Single Sign-On (SSO), enabling users who log onto the DOI network can access the Privacy Policy via the link located at the bottom of the FBMS, Enterprise Portal page or the DOI.GOV website. Users must use a PIV card and can only access



FBMS-Cloud within the DOI network. FBMS users with GrantSolutions role can access the Grants Management using FBMS Enterprise Portal or directly via the GrantSolutions website, Grantsolutions.gov.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

- Security Guards
- Key Guards
- Locked File Cabinets
- Secured Facility
- Closed Circuit Television
- Cipher Locks
- Identification Badges
- Safes
- Combination Locks
- Locked Offices
- Other.

(2) Technical Controls. Indicate all that apply.

- Password
- Firewall
- Encryption
- User Identification
- Biometrics
- Intrusion Detection System (IDS)
- Virtual Private Network (VPN)
- Public Key Infrastructure (PKI) Certificates
- Personal Identity Verification (PIV) Card
- Other. Transport Layer Security (TLS)

(3) Administrative Controls. Indicate all that apply.

- Periodic Security Audits
- Backups Secured Off-site
- Rules of Behavior
- Role-Based Training
- Regular Monitoring of Users' Security Practices
- Methods to Ensure Only Authorized Personnel Have Access to PII



- Encryption of Backups Containing Sensitive Data
- Mandatory Security, Privacy and Records Management Training
- Other

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

The Director of the Office of Financial Management is the GrantSolutions Information System Owner and is the official responsible for oversight and management of the GrantSolutions security and privacy controls and the protection of information processed and stored by the GrantSolutions system. The Information System Owner and the Privacy Act System Manager(s) are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored in GrantSolutions, and for protecting the privacy rights of the public and employees for the information they collect, maintain, and use in the system, as well as meeting the requirements of the Privacy Act, providing adequate notice, making decisions on Privacy Act requests for notification, access, amendments, and complaints in consultation with DOI Privacy Officials.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

The Director of the Office of Financial Management as the GrantSolutions Information System Owner is the official who is responsible for oversight and management of the GrantSolutions security and privacy controls, and for ensuring to the greatest possible extent that GrantSolutions data is properly managed, and that all access to data has been granted in a secure and auditable manner. The Information System Owner is also responsible for ensuring that any loss, compromise, unauthorized access or disclosure of PII is reported to DOI-CIRC, US-CERT, and Privacy officials within 1-hour of discovery in accordance with Federal policy and established procedures.