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: Enterprise Hosted Infrastructure (EHI)
Bureau/Office: Office of the Chief Information Officer
Date: September 29, 2021
Point of Contact
Name: Teri Barnett
Title: Departmental Privacy Officer
Email: DOI_Privacy@ios.doi.gov
Phone: 202-208-1605
Address: 1849 C Street NW, Room 7112, 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: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

The Enterprise Hosted Infrastructure (EHI) boundary is a General Support System (GSS) that hosts the Enterprise Directory Services (EDS). EHI provides Enterprise authentication, authorization, security, Domain Name Services (DNS), Synchronization services, and Public Key Infrastructure (PKI) services for the Department, Bureaus, and Offices utilizing Microsoft Active Directory (AD) services. EDS is a suite of services that provide authoritative enterprise level identity, authentication, and policy-based security for users and devices at the Department. EDS capabilities also include domain name services, public key infrastructure, granular delegation of permission, and security and distribution grouping.

EHI utilizes account information provided by the user to implement access control measures and rights management to ensure access to DOI's information and systems are secure. EHI is also used by other applications within DOI to perform identification and authentication on user requests to the DOI BisonConnect email system and Microsoft Office SharePoint Service (SharePoint). Providing a single directory service across DOI eliminates redundancies, standardizes configurations, and creates a more secure environment by containing access control and authentication services within one domain directory system. All subsystems within the EHI infrastructure are hosted within DOI datacenters and are non-cloud based. This is separate from the Microsoft Office 365 SharePoint Online sites, which are cloud hosted services, and is covered under the Microsoft Office 365 Cloud PIA.

The EHI PIA is being updated to reflect changes to the system. The Enterprise Hosted Service (EHS), which is the on-premise SharePoint, has been migrated to the Microsoft Office 365 Cloud boundary. Emergency Management SafeTalk, an application within the EHI boundary, was decommissioned. DOIAccess was moved to another system boundary – see the DOIAccess PIA for more information. The PIAs may be viewed on the DOI PIA website at https://www.doi.gov/privacy/pia.

The Microsoft Advanced Threat Analytics (MATS/ATA) system has been included with the EHI boundary. MATS provides security analysis of Microsoft systems and is exclusively used by authorized security and system administrative users.

C. What is the legal authority?

5 U.S.C. 301; the Paperwork Reduction Act of 1995 (44 U.S.C. 3501); the Government Paperwork Elimination Act (Pub. L. 105-277, 44 U.S.C. 3504); and Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors; E-Government Act of 2002, as amended; and 110 Departmental Manual 18. Federal Information Security Modernization Act (FISMA)

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: *Describe*

E. Is this information system registered in CSAM?

The completed PIA, associated system of records notice(s), and any other supporting artifacts must be entered into the CSAM system for each registered system or application.

☒ Yes: *Enter the UII Code and the System Security Plan (SSP) Name*

UII Code for EHI: 010-000000667
UII Code for EDS: 010-000000357
Enterprise Hosted Infrastructure (EHI) System Security and Privacy Plan

☐ 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** *If Yes, provide a description.*
Enterprise Directory Services (EDS)	Authoritative source of user identification and authentication information for DOI Enterprise.	Yes	Usernames and general contact information associated to user.
Storage Area Network	Data Storage-Record Retention stores user data, logs, records	Yes	The Storage Area Network may have information identifiable to an individual. However, any data stored is the responsibility of the program official.
Microsoft Advanced Threat Analytics (MATS)	On-premise system used to protect DOI enterprise from multiple types of advanced targeted cyber-attacks and insider threats	Yes	Monitors network traffic and collects username, system host name and IP addresses from multiple data-sources, such as logs and events for authorized network users to ensure security of the system.

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

☒ Yes: *List Privacy Act SORN Identifier(s)*

- Active Directory user accounts are covered under DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS), 72 FR 11040 (March 12, 2007). This SORN is currently being revised.
- HSPD-12 PIV user account data is covered by GSA/GOVT-7, HSPD-12 USAccess, 80 FR 64416 (October 23, 2015).

☐ No

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

☐ Yes: *Describe*
☒ No

Section 2. Summary of System Data

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

☒ Name
☒ Other: *Specify the PII collected.*

Username, password hash values, HSPD-12 authentication, official email address and phone number, duty station address, official title of DOI employees and contractors, supervisor name, Affiliation, Applicant ID, Bureau Code, Bureau Description, City, Contracting Officer Representative (COR) email, COR name, Employment Status, Network Access Required, Personal Identity Verification (PIV) Certificate, User Principal Name (UPN), Previous UPN, User Identification (UID) number, Region ID, State, Sub-Bureau Code, Sub-Bureau Description, Supervisor email, Supervisor name, and Update date. Active Directory user account information includes names, passwords, and login time, data, and locality, and is used to authenticate user access and actions within EHI. This information is used in EHI to authenticate users and is constantly synchronized through interface with AD.

The MATS system collects IP address information as part of its security scanning function. The IP addresses are only accessible via an administrative dashboard. The system is only accessible to special privileged users. IP addresses only identify individual computers and do not identify authorized users.

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: *Describe*

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

☒ Paper Format

☐ Email
☐ Face-to-Face Contact
☐ Website
☐ Fax
☐ Telephone Interview
☒ Information Shared Between Systems
☒ Other: *Describe*

EHI uses AD to authenticate users, AD user data is provided by interface with the DOIAccess Program which is located in a separate system boundary, see the DOIAccess PIA for additional information, and is also provided by individual users during the account creation or update process. Each bureau or office has their own process and forms to request and provision user accounts within AD. AD continuously updates data across the DOI domains. The EHI domain has a small number of user accounts, primarily Enterprise and Domain administrators, and is strictly controlled.

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

PII is used in the creation and administration of DOI user accounts to authenticate user access to DOI information and systems and ensure the security of DOI assets. EHI provides access control and user authentication for services, applications, and other network resources across the DOI environment using the provided information.

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

☒ Within the Bureau/Office: *Describe the bureau/office and how the data will be used.*

PII is shared with authorized personnel for the creation and administration of DOI user accounts and to provide access control and user authentication for services, applications, and other network resources across the DOI environment using the provided information.

PII may be shared with DOI law enforcement organizations for investigations of potential insider threat, violations of law, regulations or policy, or any illegal activities.

☒ Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*

User account information is replicated in all bureau/office locations and between bureau/office domain controllers for the purpose of network access enforcement, which allows all DOI users the ability to login to their assigned systems.

PII may be shared with Human Resources or DOI law enforcement organizations for investigations of potential insider threat, violations of law, regulations or policy, or any illegal activities.

☒ Other Federal Agencies: *Describe the federal agency and how the data will be used.*

PII data may be shared with federal law enforcement organizations for investigation purposes when there is an indication of potential violation of law, regulation or policy. Some information may be shared with other Federal agencies as authorized pursuant to the routine uses contained in the DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS), and GSA/GOVT-7: Personal Identify Verification Identity Management System, SORNs. Please see the SORNs on the DOI SORN website at https://www.doi.gov/privacy/sorn.

☒ Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*

Information may be shared with Tribal, state, or local agencies as authorized pursuant to the routine uses contained in the DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS), , and GSA/GOVT-7: Personal Identify Verification Identity Management System, SORNs.

☒ Contractor: *Describe the contractor and how the data will be used.*

Information may be shared with contractors who perform services or otherwise support DOI activities related to the EHI, and as authorized pursuant to the routine uses contained in the DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS), and GSA/GOVT-7: Personal Identify Verification Identity Management System, SORNs.

☐ Other Third Party Sources: *Describe the third party source and how the data will be used.*

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

☒ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

Information is voluntarily provided by employees in order to obtain access to the DOI network and information systems. Users have the opportunity to consent during the onboarding process and verification of approval to work is required to enforce access controls across the DOI network. If users decline to provide the required information upon employment at DOI they will not be given access to the network and may be unable to perform their duties.

☐ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

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

☒ Privacy Act Statement: *Describe each applicable format.*

New users are provided a Privacy Act statement during onboarding when they are issued PIV credentials. In some cases, users may request a new or updated account be created within the DOI domain through an automated form within DOIAccess that contains a Privacy Act statement.

☒ Privacy Notice: *Describe each applicable format.*

Notice is provided through publication of this PIA and the DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS), and GSA/GOVT-7, HSPD-12 USAccess, SORNs.

☒ Other: *Describe each applicable format.*

A DOI Security Warning Banner is provided to EHI System Administrators at the login screen and all network users when accessing the DOI network that informs them they are accessing a DOI system, that they are subject to being monitored, and there is no expectation of privacy during use of the system.

☐ None

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

Data is retrieved by employee or user name, workstation name, and AD group.

I. Will reports be produced on individuals?

☐ Yes: *What will be the use of these reports? Who will have access to them?*

☒ 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 from DOI records, and is not collected from other sources. User accounts are established by data provided directly from individuals during the onboarding process, which is presumed to be accurate at the time it is provided by the individual. As a function of AD, all data related to user access is continuously synchronized across the entire system.

B. How will data be checked for completeness?

Users must provide complete information during the onboarding process to establish user accounts in DOI Access and AD. Specific account attributes within EHI can be updated upon the user's request, which generally includes contact information. The specific UID information that is used to create AD user accounts is obtained from DOI Access and cannot be changed. As a function of AD, all data related to user access is continuously synchronized across the entire system.

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

Certain updates may take effect via the AD system updates, however; it is up to the individual to update their contact information and update data in any application and/or system that is hosted within EHI. DOI provides the My Account (https://myaccount.doi.gov) internal site where users can maintain and update their work related contact information. Users are notified that it is their responsibility to ensure their information is up to date. Individuals may also request access to or amendment of their records by following the procedures outlined in the applicable SORNs. As a function of AD, all data related to user access is continuously synchronized across the entire system.

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

User account records are maintained in accordance with Departmental Records Schedule (DRS) 1.4.0013, Short-term Information Technology Records, System Maintenance and Use Records (DAA-0048-2013-0001-0013), which has been approved by the National Archives and Records Administration (NARA). The disposition is temporary. Records are cut off when the employee's access has been removed, either because the employee separated, retired or transferred, or if the user's access is completely changed. Records are destroyed 3 years after cut-off. These records encompass IT files described that are not needed for extended retention. Records are characterized by being necessary for day-to-day operations but no longer-term justification of the bureaus/offices activities. In general, EHI directory configuration data is stored online 30 days on their respective servers and stored offline for 12 months. As a function of AD, all data related to user access is continuously synchronized across the entire system. Therefore, active accounts are retained within the system and the associated records will be retained for the time periods described above when user accounts are deactivated or terminated.

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

Once user accounts are terminated in the system, the records are removed in accordance with the DRS and other applicable bureau/office records retention schedules and destruction policy. Procedures for disposition of the data stored in individual applications will vary by application. When a user account is disabled or terminated in the EHI, all access will be denied since the user will no longer have the ability to log onto or authenticate to the network. The EHI user objects can be set to automatically expire at a given date to ensure that a user does not have access past the period of performance or contract. When the account is disabled, all access to the network and all EHI systems are explicitly denied and all attempts to gain access are logged. Approved disposition methods include erasing, degaussing, deleting, and shredding in accordance with the appropriate records schedule, DOI records policy and NARA guidelines.

Before purging accounts from the system, a report including the name, termination date, and a completed DI-1941, Documentation of Temporary Records Destruction form must be provided to the OS Records Office (or the bureau Records Officer) before the data is purged.

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 privacy risk to individuals due to the information contained in and used by the system, which is mitigated by controls implemented to protect data. PII used to authenticate users is limited to employee name, username, work email address, work phone number, duty station address, and official title of DOI employees and contractors. Work related PII, such as contact information, duty station, and title, is generally not considered sensitive. There is an increased risk for the management of system administrator accounts, which include username, password, and elevated privileges. System permissions and access controls are in place to limit system access to only those authorized individuals with a need to know the information to perform official functions.

There is a risk that data may be lost due to the EHS migration to the Microsoft Office 365 boundary. The data in SharePoint was migrated from the on-premise EHI SharePoint servers in DOI's datacenter to a trusted cloud instance in the Microsoft Office 365 Cloud. Data on-premise remains until transition is completed. The DOI Microsoft Office 365 Cloud system was assessed to identify privacy risk and mitigating controls, the PIA may be viewed on the DOI PIA website at https://www.doi.gov/privacy/pia.

EHI has undergone a formal Assessment and Authorization and has been granted an authority to operate in accordance with the Federal Information Security Modernization Act (FISMA) and National Institute of Standards and Technology (NIST) standards. EHI is rated as FISMA moderate based upon the type of data and it requires strict security and privacy controls to protect the confidentiality, integrity, and availability of the data contained in the system. The EHI GSS has developed a System Security and Privacy Plan based on NIST guidance and is part of a Continuous Monitoring program that includes ongoing security control assessments to ensure adequate security controls are implemented and assessed in compliance with policy and standards. Additionally, vulnerability scans are routinely conducted on the EHI GSS to identify and mitigate any found. Security and privacy awareness training are required for all DOI employees and information system users (including managers and senior executives) before authorizing access to the system, when required by system changes, and at least annually thereafter, and sign the DOI Rules of Behavior. Security and privacy role-based training are also required for employees with special roles and privileges within the system.

There is a risk that data may be inappropriately accessed or used for unauthorized purposes. Access to administrative functions is strictly controlled and can only be granted by EHI Enterprise Managers. DOI complies with NIST and other Federal requirements for data security as part of a formal program of assessment and authorization, and continuous monitoring. All information collected/contained on systems, such as MATS, is only accessible to special privileged administrators and the data is encrypted on the system drives. Monthly scans of the network are performed to ensure that changes do not occur that would create an exposure or weakness in the security configuration of any EHI equipment. The use of DOI IT systems, including EHI, is conducted in accordance with the appropriate DOI use policy. IT systems maintain an audit trail of activity sufficient to reconstruct security relevant events. The audit trail will include the identity of each entity accessing the system; time and date of access (including activities performed using a system administrator's identification); and activities that could modify, bypass, or negate the system's security controls. Audit logs are reviewed on a regular basis and any suspected attempts of unauthorized access or scanning of the system are reported immediately to IT Security.

There is a risk that data may be stored longer than necessary. Only the minimal amount of data needed to authenticate users and manage system access is collected or used, and the records are maintained and disposed of under a NARA approved records schedule. Information collected and stored within EHI is maintained, protected, and destroyed in compliance with NARA and all applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

There is a risk that individuals may not receive adequate notice of DOI privacy practices or the extent of the use of their PII data. Notice is provided to individuals through the publication of this PIA and the following SORNs: DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS) and GSA/GOVT-7, HSPD-12 USAccess. Individuals are provided privacy notice during the onboarding process and must read and acknowledge the Privacy Act Statement provided in DOIAccess, which is the Department's user credentialing system for individuals who require access to DOI networks, information systems and regular facility access. Individuals may request access to or amendment of their records by following the procedures outlined in the applicable SORNs.

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: *Explanation*

Data is required for the purposes of providing enterprise access control and management to allow seamless interaction between DOI and bureaus and offices while still maintaining the appropriate level of security.

☐ No

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

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

☒ No

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

☐ Yes: *Explanation*

☒ No

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

☐ Yes: *Explanation*

☒ No

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

Not applicable since EHI does not generate new data.

F. Are the data or the processes being consolidated?

☒ Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

Data gathered from bureaus/offices is consolidated into the DOI AD, which is used to authorize access to individual users throughout the enterprise and to manage system and application level access. EHI uses data contained within AD, and access is controlled and is only granted to a few authorized individuals with the correct level of permissions to view the data.

☐ Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐ 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
☒ Contractors
☐ Developers
☒ System Administrator
☒ Other: *Describe*

Users and contractors will have access to their own information, and in some cases a limited subset of other users based on mission, system, and application management needs.

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

Access to all EHI data will be restricted through AD permissions and access controls. System administrators will have access based on a need to know and mission accomplishment.

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. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*

The standard Privacy Act clauses are included in the contracts. The EHI contract is being updated to incorporate the most current Federal Acquisition Regulation (FAR), Privacy Act clauses and DOI Privacy policy.

☐ 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. *Explanation*

☒ No

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

☒ Yes. *Explanation*

As part of the security monitoring and management of the system, all user actions taken on EHI resources are audited and can be reviewed by Enterprise and Domain administrators. This information includes items such as: failed login/access attempts, changes in user permissions, and failed AD services associated with user authentication.

☐ No

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

As part of the security monitoring and management of the system, all user actions taken on EHI resources are audited and can be reviewed by Enterprise and Domain administrators. This information includes items such as: username, login date/time/location, failed login/access attempts, changes in user permissions, and failed AD services associated with user authentication.

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

DOI complies with NIST and other Federal requirements for data security as part of a formal program of assessment and authorization, and continuous monitoring. Monthly scans of the network are performed to ensure that changes do not occur that would create an exposure or weakness in the security configuration of any EHI equipment. The use of DOI IT systems, including EHI, is conducted in accordance with the appropriate DOI use policy. IT systems maintain an audit trail of activity sufficient to reconstruct security relevant events. The audit trail will include the identity of each entity accessing the system; time and date of access, including activities performed using a system administrator's identification; and activities that could modify, bypass, or negate the system's security controls. Audit logs are reviewed on a regular basis and any suspected attempts of unauthorized access or scanning of the system are reported immediately to IT Security.

Access to administrative functions is strictly controlled and can only be granted by EHI Enterprise Managers. Also, all users must complete IT security and privacy awareness training, as well as role-based training, on an annual basis and before being granted access, and sign the DOI Rules of Behavior.

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. *Describe*

(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. *Describe*

(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. *Describe*

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 Office of the Chief Information Officer, Enterprise Services Division, End User Services Branch Chief serves as the EHI Information System Owner and the official responsible for oversight and management of the EHI security and privacy controls for the EHI system. The Information System Owner and the AD System Manager 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 EHI. The Privacy Act System Manager is responsible for responding to Privacy Act requests 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 EHI Information System Owner is responsible for oversight and management of the EHI security and privacy controls, and for ensuring to the greatest possible extent that EHI data is properly managed and that all system access has been granted in a secure and auditable manner. The Information System Owner and all authorized users are responsible for ensuring that any loss, compromise, unauthorized access or disclosure of PII is reported to DOI-CIRC, DOI’s central incident reporting portal, within 1-hour of discovery in accordance with Federal policy and established procedures.