U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires Privacy Impact Assessments (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: Trust Evaluation System (TES)
Bureau/Office: Office of the Special Trustee for American Indians (OST), Program Management, Office of Trust Review and Audit (OTRA)
Date: December 21, 2018
Point of Contact: Associate Privacy Officer
Name: Veronica Herkshan
Title: Associate Privacy Officer (Acting)
Email: DOI_APO@ios.doi.gov
Phone: (505) 816-1645
Address: 4400 Masthead St. NE, Albuquerque, New Mexico, 87109

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 Trust Evaluation System (TES) is a web-based software application that is utilized by the Office of the Special Trustee for American Indians (OST) Office of Trust Review and Audit (OTRA) for purposes of conducting trust evaluations. TES will be hosted by a FedRAMP certified service provider who has met all requirements for information categorized as Moderate. The evaluations are critical work performed on behalf of the Secretary of the Department of the Interior (DOI) and the OST to ensure tribes and the Bureau of Indian Affairs (BIA) are in compliance with Federal regulations and fiduciary trust standards, as defined by Federal laws. Personally identifiable information (PII) is collected from authorized users and is not collected directly from the general public.

The TES will be used to collect data and documentation from tribes and the BIA to evaluate their compliance with Federal regulations, statutes, and policies in the management of Indian trust programs. Only existing information as source documentation is collected, stored or processed. The tribes and the BIA will interactively participate in the trust evaluation process by answering compliance questions, uploading documentation and submitting data to OTRA via the TES. OTRA auditors will retrieve the data and complete the evaluation. The auditors will also complete all work assignments within the TES (i.e., work papers and develop reports).

The documentation collected will include uploaded and scanned documents that may contain the names of tribes or trust beneficiaries associated with the ownership of trust assets, leases, court orders, or other trust related transactions and documentation. TES automates the communication flow between OTRA auditors, tribes, and the BIA, allowing for gains in time efficiencies and timely trust evaluation feedback.

The TES also enables efficiencies gained in the corrective action tracking process, and facilitates timely resolution of deficiencies. The use of the data contained in the TES will be used to perform administrative and mission related trust evaluation functions, which also includes evaluation management and risk planning. TES may contain PII on trust transaction documents and maintains employee information such as email addresses, positions, titles and phone numbers. OTRA creates audit case files, collects tribal and BIA data, reports and copies of source documentation.

TES will use document management capability, storage of case files, and electronic records scheduling. Users (Federal Employees and tribes) will access TES through a secured web browser. TES users will only upload source documentation in response to an audit, and will not create or enter new or additional information.

C. What is the legal authority?

The American Indian Trust Fund Management Reform Act of 1994 (P.L. 103-412), 108 Stat. 4239; 25 U.S.C. 4043; Tribal Self Governance Act of 1994 (25 U.S.C. 458cc(d)); 25 CFR 1000.350 (Trust Evaluations)

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?

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

TES UII Code: 010-000001874; TES SSP.

☐ 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.*
NONE	N/A	No	N/A

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)*

OS-02, Interior, Individual Indian Money (IIM) Trust Funds SORN, 80 FR 1043, January 8, 2015, which may be viewed on the DOI SORN website at https://www.doi.gov/privacy/os-notices.

☐ No

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

☒ Yes: *Describe*

The Office of Management and Budget (OMB) control number is #1035-0005, Tribal Evaluation System Questionnaires, Expiration date, 7/31/2021. A Privacy Act Notice is provided at the TES login screen and before access to each tribal trust program questionnaire which includes, Probate, Rights-of-Way, Residential Leases, Oil & Gas, Appraisals, Grazing, Land Title and Records Office, Forestry, Business Leases,

Acquisition & Disposals, Beneficiary Process Program, Agriculture, Sand & Gravel, Supervised Accounts, Wildland Fire, and Trust Management.

☐ No

Section 2. Summary of System Data

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

☒ Name
☒ Social Security Number (SSN)
☒ Personal Cell Telephone Number
☒ Gender
☒ Spouse Information
☒ Tribal or Other ID Number
☒ Birth Date
☒ Financial Information
☒ Medical Information
☒ Mother's Maiden Name
☒ Marital Status
☒ Disability Information
☒ Home Telephone Number
☒ Child or Dependent Information
☒ Other Names Used
☒ Truncated SSN
☒ Emergency Contact
☒ Mailing/Home Address
☒ Place of Birth
☒ Driver's License
☒ Other: *Specify the PII collected.*

Source documents may contain PII in scanned copies (not originals) of leases, probates, use and distributions plans, court ordered documentation, trust system documentation, and reports from other sources that may contain various types of PII.

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*

The system will not collect new information or any information directly from members of the public; however, the source documents may contain PII in scanned copies (not originals) of leases, probates, use and distributions plans, court ordered documentation, trust system documentation, and reports from other sources, i.e., TFAS, BIA TAAMS, Pro Trac application (Asset/Ownership data).

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: *Describe*

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

No new information is collected from individuals. The intended use of the existing PII data contained in the system will be to perform administrative and mission critical functions related to the planning of evaluations of trust programs, functions, and activities managed/administered by tribes or the BIA. Other authorized routine uses are outlined in the OS-O2, Interior, IIM Trust Funds, SORN, which may be viewed at https://www.doi.gov/privacy/os-notices.

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.*

Data/reports will be shared with OST senior management as appropriate to demonstrate compliance, or lack thereof, to trust requirements.

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

Data/reports will be shared with the BIA, Office of Self-Governance (OSG), and/or appropriate government and tribal personnel as appropriate to communicate audit results, issues and coordinate corrective actions. Data may also be shared with the Office of Inspector General (OIG) in response to, audits, evaluations and inspections by special request.

☒ Other Federal Agencies: *Describe the federal agency and how the data will be used.* Data may also be shared with the Government Accountability Office (GAO) in response to, audits, evaluations and inspections by special request, and with other Federal agencies and organizations as authorized under the Privacy Act and the routine uses published in

the OS-02 Interior, IIM Trust Funds, SORN, which may be viewed at https://www.doi.gov/privacy/os-notices.

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

Data/reports will be shared with Tribes/Consortiums that compact trust programs as appropriate to note compliance, or lack thereof, to trust requirements. Other authorized routine uses are outlined in the OS-O2, Interior, IIM Trust Funds, SORN, which may be viewed at https://www.doi.gov/privacy/os-notices.

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

Data will be shared as appropriate with the Contractor that performs the Annual Trust Funds Audit (i.e., Independent Audit of the Financial Statements for Tribal and other Trust Funds and IIM Trust Funds). Other authorized routine uses are outlined in the OS-O2, Interior, IIM Trust Funds, SORN, which may be viewed at https://www.doi.gov/privacy/os-notices.

☐ 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.*

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

OTRA does not have direct contact with individuals members of the public or Indian individuals who are the subject of the records or source documents in TES. OTRA is required to perform trust evaluations, on tribes and BIA who operate trust programs, on behalf of the Secretary (25 CFR Part 1000.350) and OST pursuant to the American Indian Trust Fund Management Reform Act of 1994, P.L. 103-412.

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.*

A Privacy Notice is posted on the TES login screen, and on the forms that collect information listed above in Section 1, Question H.

☒ Privacy Notice: *Describe each applicable format.*

Privacy Notice is provided through publication of this PIA, and the published OS-02, Interior, IIM Trust Funds, SORN at https://www.doi.gov/privacy/os-notices.

☒ Other: *Describe each applicable format.*

The DOI security banner alerts all authorized users of the system and DOI network that they are subject to monitoring and have no expectation of privacy.

☐ None

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

All information is related to official functions. Data may be retrieved by the name of a Tribe/Consortium, location, Region, Agency name, employee Auditor name, and/or an OTRA report number associated with the audit (i.e., OTRA-17-000T). No personal identifiers or PII of the subject individuals, in the copies of source records will be used to retrieve data. All contract related information (digital and hard copy) is stored and managed securely in accordance with data protection standards for contract sensitive data.

I. Will reports be produced on individuals?

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

☒ No

Reports are not produced on members of the public or individual Indians. The tribes, federal employees and auditors report on the fiduciary trust performance of trust program services, functions, or activities. OST and BIA managers may and/or will have access to the reports. Reports are produced on fiduciary trust performance of tribes and the BIA. Trust evaluation data (i.e. locations, milestone dates, hours, reports issuance dates, types of findings, and corrective action tracking milestone due dates) is collected in the process of performing the trust evaluations. These reports may include PII, but the purpose of the reports is for fiduciary trust performance, not for individuals.

Audit reports may be generated on the actions of authorized users (Audit log) for security purposes. If and actions shows unusual or malicious, etc. behavior, the logs will correlate the actions taken in the system with a username. Reports of users can be generated to include successful and unsuccessful account logon events, account management events, and privilege functions. Only system administrators and the information system owner have access to the activity reports.

Section 3. Attributes of System Data

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

The method of data collection from sources other than DOI will be verified with tribes. The tribes and the BIA shall verify information that is submitted; the data and information collected from employees and contractors will be verified and updated by Auditors during the audit report process; and, users collecting data as source documents in response to the audit questions are responsible for verifying data accuracy.

The TES application implements data input validation at entry. The user validates their information within the system. System Administrators validate data throughout the project's life cycle.

B. How will data be checked for completeness?

The tribes and BIA evaluated ("auditee's") are responsible for ensuring the completeness of data contained within the system (paper and electronic). The authorized user's are who are being audited, their data is presumed and required to be complete.

OTRA will ensure that only data related to the evaluations are used. OTRA performs a reconciliation of automated reports and hard copy or source documentation as part of the internal verification process. It is also the responsibility of the authorized users entering the data into the TES to check for completeness of the data. Authorized users are responsible for ensuring the information is correct by verifying the information with appropriate points of contact within the tribe or BIA.

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

OTRA collects data directly from tribes and BIA, as auditee's, as well as, by OTRA Auditors, so that data is presumed to be as current as possible as the time data is provided. The system will capture and store historical documentary evidence collected by scanned documents from tribes and BIA. It is the responsibility of each authorized user entering data into the TES to check for the currency of the data.

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

There have been no established retention periods for the data at this juncture. A records disposition schedule will be prepared by OST in collaboration with the OTR and submitted to the National Archives and Records Administration (NARA) for approval. Until a schedule is developed and approved by NARA, the data associated with this system will be treated as permanent records. Records may also be subject to litigation holds, court orders, and preservation notices issued by the DOI Office of the Solicitor.

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

Procedures for the disposition of the data captured within TES will be treated in accordance with NARA guidelines. Electronic records captured within TES will not be deleted or destroyed from the system, and will be disposed of in accordance with NARA guidelines and approved DOI disposition methods outlined in 384 DM 1.

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 type and volume of sensitive PII that is collected (copies of records as source documents) and maintained in the system. This risks is mitigated through administrative, physical, and technical controls that have been implemented to protect the confidentiality, integrity, and availability of the information. Privacy notice is provided to individuals through the Privacy Act notice on the TES log in screen and forms, publication of the OS-02, Interior, IIM Trust Funds SORN and this PIA. The OS-02 SORN may be viewed at https://www.doi.gov/privacy/os-notices.

There is a risk that unauthorized persons could potentially gain access to the PII maintained in the system. This risk is mitigated by restricted access to only authorized user's are allowed to enter data into the system. Only authorized user's with a "need-to-know" basis will have access to the system to perform official duties. The system is hosted on a DOI.gov website with a secure connection (HTTPS) to protect personal information of individuals records that are maintained by the system. Security and privacy controls are implemented in accordance with the Federal Information Security Modernization Act of 2014 (FISMA), the Privacy Act, OMB Circular A-130, Managing Information as a Strategic Resource, OMB Circular A-123, Management's Responsibility for Internal Control, and the National Institute of Standards and Technology (NIST) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations.

There is a risk that TES will collect more information than is necessary. This risk is mitigated by only using the minimal amount of information necessary to effectively meet the requirements for conducting tribal trust evaluations. There is a risk of maintaining inaccurate information that may result in incorrect determinations. This risk is mitigated through established quality control procedures to check the completeness of any new (existing) information that is uploaded into TES. Only authorized users are given access to be able to upload information into TES. Data that are being uploaded in response to the trust evaluations are maintained in secure DOI and contractor facilities.

There is a risk that unauthorized individuals could potentially gain access to the PII on the system. This risk is mitigated by granting access to authorized personnel and based on least privilege to perform official duties. TES is undergoing the Authorization and Accreditation (A&A) for the application and is hosted on the AWS East/West Cloud Platform, which is a FedRAMP certified cloud service provider. Users must agree to the

DOI Rules of Behavior. Electronic records are maintained in accordance with the OMB and Department guidance reflecting the implementation of the FISMA of 2014 and the Privacy Act. Electronic data is protected through user identification, passwords, database permissions and software controls, and different access levels are established for different types of users. System administrators and authorized users are trained and required to follow established internal security protocols and must complete all security, privacy, and records management training, including role-based security and/or role-based privacy training and sign the OST Rules of Behavior before authorized to access the system. The use of OST/DOI IT systems is conducted in accordance with the appropriate OST/DOI use policy. The least amount of access is given to a user to complete their required activity. All access is controlled by authentication methods to validate the authorized user.

There is a risk that some data may not be appropriate to transfer or that the contractors may not handle information according to DOI policy. TES is a cloud system rated as a FISMA moderate system and requires management, operational, and technical controls in accordance with the NIST SP 800-53 to mitigate privacy risks for the unauthorized access, disclosure, or misuse of PII. Access is limited to authorized users during the collection, use, retention, processing, disclosure, and potential destruction of information. A security plan was completed to address security controls and safeguards for the TES Cloud system. Controls are outlined in the TES Cloud System Security Plan that adhere to the standards outlined in NIST SP 800-53, Recommended Security and Privacy Controls for Federal Information Systems, and includes the use of role-based training, encryption, and maintaining data in secure facilities, among others.

An audit trail of activity will be maintained sufficient to reconstruct security relevant events. The OST follows the least privilege security principle, such that only the least amount of access is given to a user to complete their required activity. All access is controlled by authentication methods to validate the authorized user. Access to the DOI Network requires two-factor authentication. Users are granted authorized access to perform their official duties and such privileges must comply with the principles of separation of duties. Controls over information privacy and security are compliant with NIST 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations.

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*

The use of TES and the data contained in the system are relevant and necessary to perform administrative and mission critical functions, specifically to perform trust evaluations as required by Federal regulations and public law.

☐ 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?

Historical documents and source data is reconciled with hard copy source documents and system data or reports to determine relevance and accuracy.

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.*

☐ 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*

Upon request of a tribe(s) that have compacted trust functions and have been evaluated, tribes are granted authorization access to view their (respective) evaluation information only. Users supporting TES and performing system maintenance and other related activities may have access to the data in the system.

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

TES follows Governmental and Departmental standards for application access controls. All system access requires username and password authentication. All authorized users have access to view account information. Access to is limited to authorized personnel on a need-to-know basis to perform their official duties. Authorized users are trained and required to follow established internal security protocols, must complete all security, privacy, and records management training, and sign the OST Rules of Behavior. Contract employees with access to the system are monitored by the Contracting Officer Representative (COR) and OST Associate Chief Information Security Officer (ACISO).

The System administrator and supervisors are responsible for controlling and monitoring access of authorized employees. Only Authorized OST administrators and managers will receive access to data for authorized purposes.

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?*

Privacy Act contract clauses are included in all contractor agreements.

☐ 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*

☒ No

TES does not monitor individuals and members of the public. Audit logs can be used to run reports detailing an individual user's authorized access and actions performed within TES.

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

TES does not monitor members of the public. Audit logs can be used to run reports detailing an individual users' authorized access and actions performed within TES.

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

TES does not monitor members of the public. Controls outlined in the TES System Security Plan outlined in NIST SP 800-53, Recommended Security and Privacy Controls for Federal Information Systems, are in place to prevent unauthorized monitoring (of user's). This includes the use of role-based security and/or privacy training, encryption, and maintaining data in secured facilities, among others. TES assigns roles based on the principles of the least privilege and performs due diligence toward ensuring that separation of duties is in place.

Monthly scans of the network are performed to ensure that changes do not occur that would create an exposure of weakness in the security configuration of any OST assets. OST IT systems maintain an audit trail of activity sufficient to reconstruct security relevant events. 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.

Only authorized users 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. Contract employees with access to the system are monitored by the COR and IT Security.

TES is a Privacy Act System and authorized users are presented with a privacy notice and must accept the Terms and Conditions of Use each time they sign in to the application.

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*

The TES is hosted by a FedRAMP certified service provider who has met all requirements for Physical Controls for information categorized as Moderate.

(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*

In addition to the controls listed above, TES is hosted by a FedRAMP certified service provider who has met all requirements for information categorized as Moderate.

(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*

TES is hosted in AWS East/West which has Backup & Recovery and Disaster Recovery through AWS Region which has multiple, isolated locations known as Availability Zones.

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 Information System Owner (ISO) is responsible for oversight and management of the security privacy controls for the system. The Information System Owner and Information System Security Officer (ISSO), in collaboration with the Associate Privacy Officer (APO), are responsible for ensuring adequate safeguards are implemented in compliance with Federal laws and policies for the data managed and stored in the system. These officials and the Privacy Act system manager are responsible for addressing any Privacy Act requests and complaints in consultation with the APO.

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 ISO is responsible for oversight and management of the TES security and privacy controls, and for ensuring to the greatest possible extent that the data is properly managed and that all access to the data has been granted in a secure and auditable manner. The ISO is also responsible for reporting any loss, compromise, or unauthorized access to the system or data is reported DOI Computer Incident Response Center (CIRC) within 1-hour of discovery in accordance with Federal policy and established DOI procedures, and appropriate remedial activities are taken to mitigate any potential compromise in consultation with the APO.