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: OSMRE E-Budget
Bureau/Office: Office of Surface Mining Reclamation and Enforcement (OSMRE)
Date: August 15, 2023
Point of Contact
Name: Patrick Dege
Title: Associate Privacy Officer
Email: osmre_privacy@osmre.gov
Phone: 202-208-3549
Address: 1849 C Street NW, 1200W, 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?

OSMRE E-Budget (E-Budget) is an internal web-based application that is used to assist in preparation of the current fiscal year operating budget, including travel, resources, contracts, etc. The current year operating budget is populated in E-Budget at the beginning of each fiscal year along with current personnel data from the Federal Personnel and Payroll System (FPPS). Field budget Representatives review the data and add, modify, or delete transactions as needed. E-Budget is used as a "simulation tool" internally by OMSRE budget personnel to estimate an annual budget based on current criteria as well as information from prior years and then used to request current budget allocations for individual programs and offices. OSMRE E-Budget is administered by the Division of Financial Management (DFM). E-Budget does not record detail transactions, nor does it interface with any financial systems. E-Budget resides on and is a subsystem of the OSMRE Enterprise General Support System (OSMRE GSS).

C. What is the legal authority?

- The Surface Mining Control and Reclamation Act of 1977 (30 U.S.C. §§ 1201–1328)
- The Paperwork Reduction Act of 1995 (44 U.S.C. §§3501-3521) requires federal agencies to minimize the paperwork burden for individuals, small businesses, educational and nonprofit institutions, Federal contractors, State, local and tribal governments, and other persons resulting from the collection of information.
- Government Organization and Employees, Departmental Regulations (5 U.S.C. 301)
- 31 U.S.C. 331, Reports
- 31 U.S.C. 3513, Financial Reporting and Accounting System
- Federal Financial Assistance Management Improvement Act of 1999 (Public Law 106-107
- Government Paperwork Elimination Act (Pub. L. 105-277, 44 U.S.C. 3504)
- E-Government Act of 2002 (Public Law 107-347)
- Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004

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 Xacta?

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

UII Code: 010-000000721
SSPP Name: OSMRE Enterprise GSS System Security and Privacy Plan v1.6

☐ 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	None	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)*

Government personnel records are covered by OPM/GOVT-1, Government Personnel Records, 77 FR 79694, December 11, 2012, modified 80 FR 74815, November 30, 2015.

Department of the Interior (DOI) Active Directory (AD) records are covered by INTERIOR/DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS), 72 FR 11040 (March 12, 2007); Modification published 86 FR 50156 (September 7, 2021).

DOI employee administrative records are covered by INTERIOR/DOI-58, Employee Administrative Records, 64 FR 19384 (April 20, 1999); Modification published 73 FR 8342 (February 13, 2008) and 86 FR 50156 (September 7, 2021).

DOI personnel records are covered by INTERIOR/DOI-85, Payroll, Attendance, Retirement, and Leave Records, 83 FR 34156 (July 19, 2018).

These SORNs may be viewed on the DOI SORN website at https://www.doi.gov/privacy/sorn.

☐ 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
☒ Birth Date
☒ Employment Information
☒ Other: *Specify the PII collected.*

To accurately estimate budgets, personnel information is manually entered from FPPS to include name, location, date of birth (DOB), salary, benefits, and step/grade increase data. A user can only access E-Budget as a valid AD user with current and accurate credentials, an active PIV card, and a valid E-Budget user account.

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
☐ Web site
☐ Fax
☐ Telephone Interview
☒ Information Shared Between Systems: *Describe*

FPPS - Although FPPS data is used to load base information for employee costs that include name, location, DOB, salary, benefits, and step/grade increase. The information is manually entered. No information is shared electronically with any other system.

DOI AD – Username and password of OSMRE employees are used to authenticate via DOI AD to access the E-Budget system.

☐ Other: *Describe*

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

The primary use of the PII within E-Budget is to establish and manage enterprise, regional, and office level budgets in OSMRE. The information is taken from a downloaded FPPS file which includes updated OSMRE employee payroll information. This data is used by OSMRE via the E-Budget application to implement accurate budget forecasting and reporting.

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.*

Information may be shared with OSMRE Office of Planning and Budget (OPAB), Division of Financial Management (DFM), Human Resources (HR), and OSMRE program budget personnel, supervisors, or other management staff on a need-to-know basis. Request for access requires a DFM Computer Access Registration Form, which is used to track employee computer access to DFM systems, and is signed off by the person requesting access, their supervisor, their program or office budget representative, the OSMRE Budget Officer, and the DFM systems Branch Chief. Access is then granted on a granular basis with access given only to data that is required by the requesting person.

The primary use of the PII is to enable and maintain authorized access to E-Budget to accomplish business-related and mission-related budgetary management. Data is protected based on the least privilege principle. FPPS data is downloaded and then manually input into E-Budget for internal budget planning and reporting.

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

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

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

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

Contractors within OSMRE's DFM office may be involved with various aspects of E-budget such as data entry and system reporting. FAR Privacy Act clauses were included in their contract(s). Request for access requires an access form signed off by the person requesting access, their Contracting Officers Representative (COR), the program or office budget representative, the OSMRE Budget Officer, and the DFM systems Branch Chief. Access is then granted on a granular basis with only access given only to that data that is required by the requesting person.

The primary use of the PII is to enable and maintain authorized access to E-Budget to accomplish business-related and mission-related budgetary management. Data is protected based on the least privilege principles. FPPS data is downloaded and then manually input into E-Budget for internal budget planning and reporting.

☐ 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.*

The data is related to an individual's position, salary, and employment status and is necessary for normal business operations. Once you are an OSMRE employee your information will be part of the e-Budget system.

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.*

☒ Privacy Notice: *Describe each applicable format.*

Notice is provided through the publication of this PIA and the related SORNs identified in Section 1.G.

☒ Other: *Describe each applicable format.*

A warning notice that the user is entering a DOI system and to adhere to DOI policy, that there is no expectation of privacy, consent to monitoring and potential penalties is provided when a user logs in to the E-Budget system. Additionally, links are provided to DOI Accessibility Statement, DOI Disclaimer of Liability and Endorsement, FOIA, No Fear Act Reports, Cummings Act Notices, and DOI Privacy Policy.

☐ None

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

Employee name, grade, and salary information is queried through the application. Additional individual information is not required for budget calculation.

I. Will reports be produced on individuals?

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

Reports are presented by program office and include individuals within an individual program. This information is used by managers and administrative staff for budgetary purposes including percentage award amounts on salaries at the end of the year. Supervisors can request these reports for their program area from Human Resources or their budget representative.

☐ No

Section 3. Attributes of System Data

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

The information is taken from DOI records in FPPS. Data is not collected from other sources. Should data be entered erroneously into E-Budget notice would be given to the E-Budget program office by the discoverer for manual correction in the system. Should there be an error within the FPPS data itself, correction would follow the Interior Business Center (IBC) process for the FPPS system starting with notice to the IBC FPPS program office.

B. How will data be checked for completeness?

The information from FPPS is verified that all fields are complete at the time of download. Should there be an error within the FPPS data itself, correction would follow the IBC process for the FPPS system starting with notice to the IBC FPPS program office.

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

E-Budget data is downloaded from IBC's FPPS system and is current for the fiscal year and is deemed reliable at the time it is downloaded. However, the system performs validation and reconciliation of information at each system interface to ensure that the data is transferred and stored properly, without data validation errors.

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

Data and potential records within the E-Budget system are included under the DFM files maintenance and disposition plan under records authority DAA-0048-2013-0001 and scheduled under DRS 1.3.A.10 as Short-term Financial and Acquisition Records. These records are considered temporary and are to be cut off at the end of the FY in which the record is created then destroyed 3 years after cut-off.

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

Approved disposition methods include shredding, burning, or pulping paper records, and degaussing or erasing electronic records in accordance with Department policy and NARA guidelines. However, data (electronic and paper) files transferred to the Federal Record Center (FRC) are disposed of via methods determined by the FRC.

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 employee data that may be maintained in the E-Budget system. However, PII data is restricted to employment related information and is ultimately Freedom of Information Act accessible. E-Budget, as a part of the OSMRE GSS, inherits mitigating controls implemented to protect data and substantially lower privacy risks. The protection and maintenance of information for recovery and backup purposes is done following OSMRE policy and process for backup and retention of information. System permissions and access controls are in place to limit system access to only those authorized individuals with the proper authorization to perform official functions.

There is nominal risk to the privacy of official user information throughout the information lifecycle; user information is authenticated by AD for access to E-Budget. Risk is further reduced by following established guidance from NIST SP 800-53 on access controls. Privacy risk to E-Budget accounts would include usernames, passwords and security questions and answers through the OSMRE GSS. These risks are mitigated by a combination of administrative, physical, and technical controls. E-Budget inherits a Moderate system security categorization as a part of the OSMRE GSS in accordance with National Institute of Standards and Technology (NIST) standards and Federal Information Processing Standard (FIPS) 199, and the Federal Information Security Modernization Act (FISMA).

There are privacy risks related to hosting, processing, and sharing of data, unauthorized access to records, or any inappropriate use and dissemination of information. These risks are mitigated through a combination of physical, administrative, and technical controls, inherited as a subsystem of the OSMRE GSS. Risk is also mitigated through system configuration controls that limit or prevent access to privacy information. The OSMRE GSS utilizes appropriate security and privacy controls implemented to safeguard information collection, use, retention, processing, disclosure, destruction, transmittal, storage, and audit logging. It covers access controls, password management, firewalls, segregation of duties, and encryption of database, media, and communications. The OSMRE GSS and E-Budget systems utilize the principle of least privilege access for authorized users to perform their duties. The OSMRE GSS Information System Continuous Monitoring Plan (ISCMP) specifies the review, monitoring and assessment frequency of all NIST Special Publication (SP) 800-53 security and privacy controls to maintain the integrity and accuracy of the data. Federal government information is managed and safeguarded by following NIST, FISMA, OSMRE, and DOI security and privacy policies. All access is controlled by authentication methods including multi-factor authentication (MFA) utilizing Personal Identity Verification (PIV) cards to validate authorized users. All DOI employees and contractors are required to complete annual security and privacy awareness training and sign DOI Rules of Behavior. Personnel authorized to manage, use, or operate the E-Budget application are required to take additional role-based privacy and security training annually. E-Budget data is under the control of the DFM Branch Chief, who is responsible for protecting the privacy rights of the individuals whose information they collect, maintain, and use, and for meeting the requirements of the Privacy Act, including providing adequate notice, making decisions on Privacy Act requests for notification, access, and amendments, as well as processing complaints, in consultation with OSMRE and DOI privacy officials. The DOI Privacy Program website also contains DOI privacy officials' contact information and provides guidance to individuals on how to submit requests or complaints under the Privacy Act.

DOI Active Directory (AD) and network infrastructure provides information and services for the purpose of authenticating users and managing access. Initial information is collected by Human Resources (HR) or the Contracting Officer Representative (COR) from individuals during the on-boarding process to establish user accounts. As part of this process, the individual is instructed to complete required Information Management and Technology (IMT) Awareness training in security, privacy, records management, Section 508, Controlled Unclassified Information, and Paperwork Reduction Act. Additionally, the user is required to agree to the DOI Rules of Behavior (RoB). HR then creates a request which notifies authorized personnel to create the network account(s) for OSMRE GSS. This information is managed in DOI AD and is not collected by OSMRE GSS or the E-Budget system. IMT training must be repeated and the RoB's attested to on an annual basis by all OSMRE employees and contractors.

There is a risk that unauthorized persons could potentially gain access to the PII on the system or misuse the data. To mitigate this risk, access to data is restricted to authorized personnel who require access to perform their official duties. Technology is employed to protect information in transit using both server authentication and data encryption. Platform and device level encryption have been deployed to encrypt data at rest. Other security mechanisms have also been deployed to ensure data security, including but not limited to, firewalls, virtual private network, and intrusion detection.

There is a risk that user PII may be inappropriately used or disseminated by personnel authorized to access the system or view records. The system uses audit logs to protect against unauthorized access, changes, or use of data. OSMRE employees and contractors are required to take annual mandated security, privacy, and records management as well as role-based privacy and security training where applicable, and sign DOI Rules of Behavior prior to accessing E-Budget. Additionally, request for access requires an access form signed off by the person requesting access, their supervisor, their program, or office budget representative, the OSMRE Budget Officer, and the DFM Branch Chief. Access is then granted on a granular basis with access only given only to that data that is required by the requesting person. Failure to protect PII or mishandling or misuse of PII may result in disciplinary actions and potential termination of employment, criminal, civil, and administrative penalties.

There is a risk that users may not receive adequate notice of the purpose and uses of their information. This risk is mitigated by the publication of this PIA, applicable SORNs, and the warning notice posted when entering a DOI system. Links are also provided to the DOI Privacy Policy, DOI Accessibility Statement, DOI Disclaimer of Liability and Endorsement, FOIA, etc.

There is a risk that erroneous information may be collected. This risk is mitigated by restricting data collection to official FPPS records of DOI accounts. Should data be entered erroneously into E-Budget, notice would be given to the E-Budget program office by the discoverer for manual correction in the system. Should there be an error within the FPPS data itself, correction would follow the IBC process for the FPPS system starting with notice to the IBC FPPS program office.

There is a risk that information in the system will be maintained longer than necessary to achieve the bureaus mission or may be improperly disposed or destroyed. This risk is mitigated by maintaining and disposing of records in accordance with records retention schedules approved by NARA. Users are reminded through policy and training that they must follow the applicable retention schedules and requirements of the Federal Records Act. Contingency plans and procedures are defined to ensure the ability to recover in the event of improper data disposal.

OSMRE complies with DOI, NIST, and other Federal requirements for data security as part of a formal program of assessment and authorization, and Continuous Diagnostics and Mitigation (CDM) 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 network equipment. The use of OSMRE IT systems, including E-Budget, is conducted in accordance with the appropriate OSMRE and DOI use policy. OSMRE IT systems maintain an audit trail of activity sufficient to reconstruct security relevant events. The audit trail includes 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 OSMRE IT Security and the DOI OCIO. Access to administrative functions within E-Budget is strictly controlled and can only be authorized by E-Budget program managers.

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 collected is required to provide services to efficiently manage budgetary and salary data for effective budgetary management within OSMRE and in support of the OSMRE mission.

☐ 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?

N/A - The information is taken directly from DOI records in FPPS and 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. *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*

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

Access is granted on request by supervisor and approved by the OSMRE budget office and the system owner. Current OSMRE and DOI Rules of Behavior apply to access and use of data.

Access granted to authorized personnel is enforced with PIV card, MFA, and password using the least privilege principle. Request for access requires an access form signed off by the person requesting access, their supervisor (or Contracting Officers Representative (COR) in the case of contractors), the program or office budget representative, the OSMRE Budget Officer, and the DFM Branch Chief. Access is then granted on a granular basis with only access given only to that data that is required by the requesting person.

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?*

Contractors may be involved in carrying out authorized design and configuration in the E-Budget system. The E-Budget System Owner is responsible for approving all contractor led design, testing, deployment, and maintenance under contractor control, and must adhere at all times to all Federal laws, regulations, OMB, Department of Homeland Security (DHS) and DOI policies, directives, and memorandums. Privacy Act Federal Acquisition Regulations contract clauses are included in all contractor agreements in accordance with, and subject to, the Privacy Act of 1974, as amended, 5 U.S.C. 552a, and applicable OSMRE and DOI regulations. Current contracts not in compliance with the Information Technology (IT) Baseline Compliance Contract Guidelines memorandum of August 15, 2022, will be modified to comply.

☐ 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*

The purpose of the E-Budget system is not to monitor individuals; however, user actions and use of the system are logged via system logs for security purposes in accordance with OMB, DHS and DOI policies, directives, and memorandums. Information captured include, but is not limited to username, user's last date of login, date of user content creation, date user content was modified or deleted. Additionally, the DOI security network tools include routers, firewalls, and software that log and establish an audit trail of creation and modification of user actions, and the date and time the actions took place. Logs are only accessed by authorized administrative/manager staff.

☐ No

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

The system does not actively monitor E-Budget users and is not programmed to do so. Audit logs are maintained in the system and track login attempts and errors. Audit logs record username, date/time, actions. Information collected is used to monitor user access (username) and activity (logins, record changes, deletions, additions, date, and timestamp) for auditing purposes.

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

Access to the E-Budget is only provided to authorized personnel and is applied on the principle of least privilege in order to manage access and log events. Audit features track user activity and record all changes. E-Budget complies with all OMB, DHS, and DOI policies, directives and memorandums that are incorporated into the Assessment and Authorization to Operate (ATO) of the OSMRE GSS.

The E-Budget system, through the OSMRE GSS, maintains an audit trail of activity sufficient to reconstruct security-relevant events. Audit trails 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 as required, and any suspected attempts of unauthorized access or scanning of the system is reported immediately to OSMRE IT Security. Access to administrative functions is strictly controlled. Additionally, users must be included in individual security groups assigned to specific resources to access that particular resource.

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 DFM Branch Chief serves as the E-Budget System Owner and the official responsible for oversight and management of the E-Budget security controls and the protection of agency information processed and stored by the E-Budget system. In addition, the Chief, Mission System Support Branch, as System Owner for the OSMRE GSS on which the E-Budget application resides, is also responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies, as well as processing complaints, in consultation with the OSMRE Associate Privacy Officer (APO).

The E-Budget System Owner is responsible for protecting the privacy rights of the individuals whose information they collect, maintain, and use in each system, and for meeting the requirements of the Privacy Act, including the reporting the loss, compromise, unauthorized disclosure, or access of individuals' personal information, in consultation with the OSMRE APO.

The OSMRE Incident Response Team handles incidents in accordance with OSMRE incident response policy and the DOI Privacy Breach Response Plan, which provides guidance on breach response, the process for timely notification to individuals, and other remedial actions.

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 E-Budget System Owner is responsible for oversight and management of the E-Budget security and privacy controls, and for ensuring to the greatest possible extent that E-Budget is properly managed, and that access is granted in a secure and auditable manner. The E-Budget System Owner is also responsible for ensuring that any loss, compromise, unauthorized access, or disclosure of PII is reported to the OSMRE APO and the OSMRE Incident Response Team in accordance with the DOI Privacy Breach Response Plan and the OSMRE Incident Response Plan. System administrators, employees and contractors are required to report any potential loss or compromise to the E-Budget System Owner, Information System Security Officer and the OSMRE APO.