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.

Name of Project: Office of Government Ethics, Integrity Application
Bureau/Office: Office of the Secretary/Office of the Solicitor
Date: October 27, 2021
Point of Contact:
Name: Danna Mingo
Title: OS Departmental Offices Associate Privacy Officer
Email: OS_Privacy@ios.doi.gov
Phone: (202) 208-3368
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

B. What is the purpose of the system?

Integrity is an Office of Government Ethics (OGE) owned and managed secure public web facing electronic financial disclosure reporting system used by Executive branch agencies. Integrity collects, manages, processes, measures, and stores financial disclosure information from certain Federal employees and members of the public in anticipation of nomination by the President and approval by the Senate, through OGE Form 278e and OGE Form 278-T for the purpose of identifying, preventing, and

resolving conflicts of interest in accordance with Ethics in Government Act of 1978 and the Ethics Reform Act of 1989, as amended, and Executive Order (E.O.) 12674 as modified.

The Department of the Interior (DOI) has entered into an agreement with OGE to use Integrity for all DOI OGE 278 public financial disclosure reporting. DOI will use Integrity to automate the annual financial disclosure process required for Federal employees and other individuals to fulfill their obligations and requirements to file annual financial disclosure reports. Integrity helps the Departmental Ethics Office within the DOI Office of the Solicitor ensure compliance with Federal conflict of interest laws, and regulations and requirements to preserve and promote the integrity of public officials and institutions.

The OGE Integrity system is used by Federal agencies and utilizes the Office of Management and Budget (OMB) MAX Platform-as-a-Service to manage access controls. Integrity is hosted in a U.S. Government agency cloud by the U.S Department of Agriculture (USDA), National Information Technology Center (NITC), an authorized Federal Risk and Authorization Management Program (FedRAMP) cloud service provider.

OGE is the Integrity System Owner and is responsible for oversight and management of Federal Government use of Integrity. OGE has conducted a privacy impact assessment (PIA) to assess privacy risks related to OGE use and operation of Integrity, which may be viewed on the OGE PIA page at https://www.oge.gov/Web/OGE.nsf/resources/privacy+impact+assessments. The Department of the Interior (DOI) is a Federal agency user of Integrity and is responsible for oversight, creation and management of DOI accounts, use and access controls, training, and retention and disposal of DOI records in Integrity. DOI is conducting this PIA to evaluate privacy risks related to DOI's use of the OGE Integrity system and the collection, storage, use, processing, disclosure and disposal of personally identifiable information (PII) about DOI employees and members of the public.

C. What is the legal authority?

Stop Trading on Congressional Knowledge Act of 2012 (STOCK Act), Pub. L. 112–105, as amended; Ethics in Government Act of 1978), 5 U.S.C. app. §§ 101, 103(l); 5 U.S.C. 7301, 7351, 7353; 31 U.S.C. 1353; Executive Order 12674 (as modified by Executive Order 12731);

5 CFR Part 2634, Subpart I, of the Office of Government Ethics regulations; 5 CFR Part 3501--Supplemental Standards of Ethical Conduct for Employees of the Department of the Interior; 43 CFR Part 20--Office of the Secretary of the Interior, Employee

Responsibilities and Conduct; OGE Program Advisory PA-15-01, Implementation of Integrity and New Public Financial Disclosure Report Form.

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

Integrity is an OGE owned and managed system. OGE and DOI have entered into an agreement for DOI to use Integrity to manage annual public financial disclosure reporting.

E. Is this information system registered in CSAM?

☒ Yes

Integrity is registered in CSAM under the Office of Government Ethics, Integrity Application (OGE - Integrity) and DOI is leveraging the OGE Integrity System Security Plan for DOI's authorization to use Integrity. A UII Code is not required for the Integrity System.

☐ 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	Describe
None			

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

☒ Yes

The information in this system is covered under the following SORNS: OGE/GOVT-1, Executive Branch Personnel Public Financial Disclosure Reports and Other Name-Retrieved Ethics Program Records, 84 FR 47303 (September 9, 2019) and OGE/GOVT-2, Executive Branch Confidential Financial Disclosure Reports, 84 FR 47301 (September 9, 2019). The SORNs can be reviewed at the following url: https://www.fpc.gov/resources/SORNs/#container

☐ No

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

☒ Yes

The forms are owned by the US Office of the Government Ethics and they are responsible for the OMB approval requirements.

☐ No

Section 2. Summary of System Data

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

☒ Name
☒ Spouse Information
☒ Financial Information
☒ Personal Email Address
☒ Group Affiliation
☒ Marital Status
☒ Child or Dependent Information
☒ Employment Information
☒ Mailing/Home Address
☒ Other

Integrity contains information on filers who complete public financial disclosure reports including name, agency, official position, address, phone number, email address, reportable financial information required under the Ethics in Government Act of 1978. Information may also include work grade/title; work phone; type of filer; types and amounts of non-Federal salaries, investments, and assets; who holds the asset or investment (no identifying information is collected about spouse or child); creditors – names and addresses; personal and family holdings; other investments/interests in property; salary; dividends; retirement benefits; deposits in banks and other financial

institutions; information on gifts received; information on certain liabilities; information about positions as an officer, director, trustee, general partner, proprietor, representative, employee, or consultant of any corporation, company, firm, partnership, or other business, nonprofit organization, labor organization, or educational institution; information about non-Government employment agreements, such as leaves of absence to accept Federal service, continuation of payments by a non-Federal employer; information about assets placed in trust pending disposal and other information related to conflict of interest determinations; names of other employers; and name of Congressional committee considering a nominee if the filer is a Presidential nominee. Filers may also optionally provide a personal or home telephone number, personal email address, and/or a personal or home mailing address.

Personal email address, mailing address, and telephone number is collected for OGE Form 278e filers who are not at DOI at the time they file the disclosure--this includes filers who file termination reports after leaving government service. For authorized users who are not filers, Integrity requires the user's name, agency, system role(s), access permissions, official address, official telephone, and official email address.

Records in this system may also include information from supporting documents and other sources provided during reviews. See the OGE/GOVT-1 government-wide system of records notice for categories of records maintained in this system. Integrity only collects information from OGE Form 278e and is not intended to be a records management system for other DOI Ethics Program documents such as Certificates of Divestiture, ethics pledge waivers, ethics agreements, and waivers issued pursuant to 18 U.S.C. §§ 208(b)(1) and (b)(3).

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

Individual filers provide information when they report personal or financial disclosure information. Information may be provided to or by Executive branch agencies when individual filers transfer to or from DOI.

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

Information is primarily collected from individual filers electronically through OGE Form 278e on the secure Integrity website at https://www.integrity.gov/efeds-login/. Additional information or supporting documentation may be provided through email or paper or other medium during interviews or follow up with individual filers.

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

Individual filers are required to provide their contact information, such as agency, business address, telephone number and official email address. Filers using the system provide their official position title and reportable personal financial information. The information collected is used to facilitate the annual financial disclosure process pursuant to the Ethics in Government Act of 1978 and the Ethics Reform Act of 1989, as amended, and E.O. 12674 as modified. OGE requires certain employees and members of the public, usually nominees to Presidentially-appointed, Senate-confirmed (PAS) positions, or terminated PAS officials, to file financial disclosure reports to avoid involvement in a real or apparent conflict of interest. The purpose of the financial disclosure reports is to assist employees and agencies in identifying, preventing, resolving and avoiding conflicts of interest between their official duties and their private financial interests or affiliations.

The information provided will only be used for legitimate purposes and will be disclosed to any requesting person as authorized by law in accordance with 5 CFR 2634.603. The OGE Form 278e is a publicly available document. A member of the general public may request a copy of the OGE Form 278e by using OGE 201 Form: Request to Inspect or Receive Copies of Executive Branch Personnel Public Financial Disclosure Reports or Other Covered Records. The DOI Ethics Office has 30 days to comply with an OGE Form 201 application.

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

☒ Within the Bureau/Office

Individual filers have access only to their own records in the system. Certain Departmental Ethics Office (DEO) senior ethics officials have the ability to view all OGE 278e forms or DOI records within Integrity. Other DOI ethics officials only have the ability to view the forms that have been assigned to them. Bureau Deputy Ethics Counselors see all forms submitted by their bureau employees (filers) – they do not see other Bureau forms or the DEO forms. These forms are used only for review by DOI ethics officials to determine compliance with applicable Federal conflict of interest laws and regulations.

☒ Other Bureaus/Offices

Reports may be shared with the Office of Inspector General for the purposes of conducting an authorized inquiry or audit. Information may be shared with another bureau if an employee transfers to a new bureau.

☒ Other Federal Agencies

The OGE has access to the information to perform their oversight functions, submit required reports on annual OGE Form 278e filers, and ensure compliance with the Ethics in Government Act of 1978 and the Ethics Reform Act of 1989, as amended, and E.O. 12674 as modified. If an employee who files an OGE Form 278e or OGE 278-T transfers to another Federal agency into another position that requires the filing of the OGE Form 278, the employee and/or new Federal agency may request a copy of the OGE Form 278e and OGE 278-T that was submitted by the filer. Information may be shared with the U.S. Government Accountability Office for accounting and oversight purposes, the Department of Justice in connection to litigation related to ethics matters, and with other agencies and organizations as authorized and consistent with the routine uses published in the applicable government-wide OGE/GOVT-1 system of records notice.

☐ Tribal, State or Local Agencies

☒ Contractor

Only DOI Federal employees are system administrators for the DOI use of the Integrity system. However, information may be shared with contractors performing work under contract to the Federal government to provide support for authorized purposes or for system operation, administration and maintenance purposes.

☒ Other Third-Party Sources

The OGE Form 278e is a publicly available document. In accordance with 5 CFR 2634.603, a member of the general public may request a copy of the OGE Form 278e by using OGE 201 Form: Request to Inspect or Receive Copies of Executive Branch Personnel Public Financial Disclosure Reports or Other Covered Records. DOI Ethics officials have 30 days to comply with an OGE Form 201 application.

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

☒ Yes

Filers are made aware of public financial disclosure filing requirements as part of the recruitment process via statements in vacancy announcements. Filers are further notified during in-processing briefings by their Human Resources department representatives. Privacy Act Statements are provided to filers on the OGE Form 278e and Form 278-T and on the Integrity website Privacy Policy informing individuals of the authority, purpose, uses, and disclosures of their information. Individuals may decline to complete the financial disclosure forms or provide the required information. However, there are penalties for Federal employees and other consequences for individuals who do not complete their financial disclosure reports or otherwise meet the requirements under the Ethics in Government Act of 1978, Executive Order 12674 and 5 CFR 2634 Subpart 1 of the Office of Government Ethics, which require the reporting of this information. Failure to provide the requested information may result in fines, separation, disciplinary action, or prosecution.

☐ No

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

☒ Privacy Act Statement

A Privacy Act Statement is provided on OGE Form 278e, OGE Form 278-T, and in the Integrity Privacy Policy posted on the Integrity website. Filers are made aware of financial disclosure filing requirements as part of the recruitment process via statements in vacancy announcements. Filers are further notified during in-processing briefings by their Human Resources representatives.

☒ Privacy Notice

Notice is provided to individuals through the publication of this PIA, the OGE Integrity PIA available on the OGE PIA web page at https://www.oge.gov/Web/OGE.nsf/resources/privacy+impact+assessments, and the published OGE/GOVT-1, Executive Branch Personnel Public Financial Disclosure Reports and Other Name-Retrieved Ethics Program Records, 84 FR 47303 (September 9, 2019) and OGE/GOVT-2, Executive Branch Confidential Financial Disclosure Reports, 84 FR 47301 (September 9, 2019) SORNs. The SORNs can be reviewed at the following url: https://www.fpc.gov/resources/SORNs/#container

☒ Other

The Integrity login page on the OMB MAX.Gov website displays a warning banner to users.

☐ None

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

Ethics officials log into Integrity to view, certify or retrieve forms by specific employee or filer name, and can also retrieve records by the organization or the form type (OGE Form 278-T or OGE Form 278e).

I. Will reports be produced on individuals?

☒ Yes

DOI Ethics officials use Integrity to view and certify OGE Form 278e and OGE Form 278-T submitted by individual filers to determine compliance with applicable Federal conflict of interest laws and regulations. Reports may be generated to show the processing status or review status (e.g., assigned, draft, under review or certified) of DOI filers and annual reports. Reports will also show individuals who have filed their OGE forms and those individuals who have not filed their forms. Reports may include a list of names and work or personal email addresses for current or former employees who left the agency and still need to file a financial disclosure report. DOI Ethics officials use this information to ensure compliance with Federal requirements and it may be shared with DOI employees' supervisors in order to get the employees to file the required forms. Comprehensive reports may also be generated in Integrity to list all filers that include names and email addresses. There are no reports that pull, extract, or compile sensitive or financial information from the actual OGE Form 278-T or OGE Form 278e

submitted by individuals. OGE has access to Integrity information and processing status information for all agencies.

☐ 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 through OGE Forms 278e and 278-T from individual filers and is verified by DOI Ethics officials through oversight procedures established by OGE to ensure compliance with the Ethics in Government Act of 1978, Executive Order 12674 and 5 CFR 2634 Subpart 1 of the Office of Government Ethics. Any discrepancy or information found is shared with the filer to verify accuracy of the information. Individual filers are responsible for ensuring accuracy of PII data they provide and are required to certify to this effect.

B. How will data be checked for completeness?

It is the individual filer's responsibility to ensure the information provided in their financial disclosure reports is complete and accurate. Integrity includes required fields functionality to ensure filers complete all fields required for OGE Form 278-T and OGE Form 278e. Integrity will generate an error message and highlight incomplete required fields. Thereafter, DOI Ethics officials review the form for completeness and make further inquiries of the filer if needed.

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

It is the individual filer's responsibility to ensure the information provided in their financial disclosure reports is updated and remains current. The information in Integrity is kept current through mandatory annual updates by the employees and filers. Some filers may be required to submit an updated financial disclosure report within 30 days of a change as required under the STOCK Act. OGE regulations require certain Federal employees to file OGE Form 278e and OGE Form 278-T, and these employees submit updated forms annually as long as the employees remain in a position that requires filing.

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

The DOI Ethics Office has overall responsibility for managing and properly disposing of all DOI records collected and maintained in Integrity. Records disposal is carried out by

authorized DOI Ethics officials. DOI Ethics program records are currently included under the National Archives and Records Administration (NARA) General Records Schedule (GRS) 2.8: Employee Ethics Records. This schedule outlines records retention for general ethics program records, referrals and notifications of conflict of interest/other violations, reports of payments, questionnaire records, ethics program reviews, ethics agreements, and financial disclosure records.

NARA sets different records retention for various categories of records under this schedule. General ethics program records for the coordination and management of agency ethics programs must be destroyed 6 years following the closure of the document/completion of the purpose for which it was created (e.g., conclusion of ethics regulatory review, making determination regarding outside employment, etc.). This authority is cited as GRS 2.8 - 010 (DAA-GRS-2016-0006-0001).

Records retention for public financial disclosure reports ranges by item (GRS 2.8 - 060, 061, 062, and 063).

- OGE Form 278e public financial disclosure reports and related records are destroyed 6 years after receipt by the agency (DAA-GRS-2014-0005-0008).
- For officials not confirmed by the U.S. Senate, in all cases, the records must be destroyed 1 year after the nominee ceases to be under consideration (DAA-GRS-2014-0005-0007).
- For periodic transaction reports (OGE 278-T), records must be destroyed 7 years after receipt by the agency, or when the related Form 278 is ready for destruction. (DAA-GRS-2014-0005-0009).
- Requests to inspect or receive copies of executive branch personnel public disclosure reports or other records must be destroyed when the requested report is destroyed (DAA-GRS-2014-0005-0010).

The GRS provides specific authorities that can be cited for all categories of records. Please see: https://www.archives.gov/files/records-mgmt/grs/grs02-8.pdf

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

DOI Ethics Program officials are responsible for disposing of DOI records at the end of their retention period in Integrity. The OGE Form 278e remains in the system for a period of six (6) years, then are purged or destroyed, and periodic transaction reports (OGE 278-T) records are destroyed 7 years after receipt by DOI in accordance with GRS 2.8 and OGE regulations unless the DOI Ethics official is notified by the Office of Inspector General that the individual is under investigation and to keep the report until the investigation is complete. Integrity system user activity and event logs are configured to automatically overwrite the oldest activity and event once the activity or event storage capacity is reached. Approved

disposition methods include shredding or pulping for paper records, and degaussing or erasing for electronic records, in accordance with NARA Guidelines and 384 Departmental Manual 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 amount of PII collected, used and maintained in the Integrity system. This risk is mitigated through administrative, technical and physical controls implemented by OGE and DOI to safeguard the confidentiality, integrity and availability of information and the Integrity information system.

OGE contracted with the U.S. Department of Agriculture National Information Technology Center (NITC) to host the Integrity servers. NITC is Federal Risk and Authorization Management Program (FedRAMP) authorized as a cloud service provider that has met all requirements for Integrity for information categorized as Moderate in accordance with the Federal Information Security Modernization Act of 2014 (FISMA). OGE has conducted a formal Assessment and Authorization and issued an authority to operate for the Integrity system in accordance with FISMA and National Institute of Standards and Technology (NIST) standards and guidelines. Integrity follows NIST criteria for categorization, selection, development, implementation, assessment, authorization, and monitoring of security controls.

OGE and DOI have entered into an agreement for DOI's use of Integrity that includes provisions pertaining to the handling, sharing, and retention of relevant data designed to ensure privacy and data protection. As the managing agency, OGE is responsible for ensuring the Integrity system management, operational, and technical controls established by NIST SP 800-53 are in place to mitigate the security and privacy risks for Federal agency use of the system. As a Federal agency user, DOI has reviewed the OGE Integrity authorization package for issuance of an Authority to Use (ATU) for the Integrity system. DOI has ownership and control of DOI records in the DOI instance of Integrity and is responsible for ensuring adequate security and privacy controls are implemented to prevent unauthorized access or disclosure.

There is a risk of unauthorized access to the Integrity system and data. The Integrity system follows strict security and privacy controls to protect the confidentiality, integrity, and availability of data in the system at the moderate level. Integrity grants access to the system based on least privilege principle, role-based approach for user account authorization and access enforcement. System users access the Integrity using MAX.Gov via a secure Hypertext Transfer Protocol Secure (HTTPS) connection. In addition to physical controls, operational and technical controls in place

to limit these risks include firewalls, encryption, malware identification, and periodic verification of system users. Ports and services that are not needed are disabled in the operating system, servers are patched and updated regularly. Firewalls and Intrusion Detection Systems (IDS) monitor and block unauthorized connections. Servers use current antivirus software to check for viruses in real time and logs are routinely checked for unauthorized access or server problems. All communications between Integrity servers and the user's desktop/laptop computers are encrypted during transmission. Data is encrypted during transmission and at rest then stored on Federal government owned and operated computer systems in secured database with restricted access. Access controls and system logs are reviewed regularly as part of the FedRAMP continuous monitoring process. Hard copy documents containing PII are secured in a locked office, desk drawer or file cabinets. NITC is subject to all the Federal legal and policy requirements for safeguarding Federal information, and is responsible for preventing unauthorized access to the system and protecting the data contained within the system. Integrity stores all data in a secure database and access and has met DOI's information system security requirements, including operational and risk management policies.

There is a risk information in the Integrity system may be used for an unauthorized purpose or outside the scope of what it was originally intended when it was collected. The DOI Ethics Office approves the officials requesting access to restricted Integrity folders to those who have a valid need-to-know and monitors permissions on an ongoing basis. DOI Integrity system users are required to take annual DOI security, privacy, and records management training and also sign a DOI Rules of Behavior Agreement prior to accessing DOI information or information systems. Federal and non-Federal users read and acknowledge Integrity system Rules of Behavior and User Agreement provided on the Integrity system landing page prior to accessing Integrity: https://www.integrity.gov/efeds-login/. Also, all DOI Ethics officials and supervisors who review these documents are required to take security and privacy training and keep filers' personal information strictly confidential.

There is a risk that individuals may not have notice of the purposes for collecting their information, including how it will be used. Individual filers are notified of the privacy practices through this PIA, the OGE Integrity PIA, the published Government-wide OGE/GOVT-1 SORN, detailed Privacy Act Statements on the OGE Forms 278e and 278-T and the Integrity website Privacy Policy, and disclosures during the recruitment and onboarding process.

There is a risk that erroneous information concerning filers may be stored in the system. In an effort to increase accuracy, information is collected directly from filers during the hiring and on-boarding process, as well as annual submission of financial disclosure forms. It is the individual filer's responsibility to ensure the information they provide in their financial disclosure reports is accurate and current. Per OGE regulations,

filers' financial disclosure reports shall be taken at "face value" as correct, unless there is a "patent omission or ambiguity or the official has independent knowledge of matters outside of the report." A filer may initiate an amendment to report, a reviewer may make the amendment directly, either based on additional information from the filer or independent knowledge.

There is a risk of over-collection of PII or financial information from filers. The amount of financial data requested from individuals is required so DOI Ethics Officials can thoroughly review reports for possible conflicts between official duties and private financial interest or affiliations to ensure compliance with the Ethics in Government Act of 1978, Executive Order 12674 and 5 CFR 2634 Subpart 1 of the Office of Government Ethics, which require the reporting of this information. DOI does not collect Social Security numbers, dates of birth or unnecessary personal information from filers or maintain them in Integrity.

There is a risk that PII information may be retained for longer than necessary. In regards to information handling and retention procedures, DOI is responsible for managing and disposing of DOI records in Integrity as the information owner. DOI ensures records are not needed for investigation then destroys them in accordance with records retention schedules approved by NARA, GRS 2.8: Employee Ethics Records. Information collected and stored within Integrity is maintained, protected, and destroyed in compliance with all applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

Section 4. PIA Risk Review

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

☒ Yes

Integrity is a solution for automating the annual public financial disclosure process. Integrity facilitates the automation of OGE Form 278-T and Form 278e.

☐ No

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

☐ Yes

☒ No

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

☐ Yes

☒ No

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

☐ Yes

☒ No

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

Not applicable

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated.

☐ Yes, processes are being consolidated.

☒ No, data or processes are not being consolidated.

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

☒ Users
☒ Contractors
☐ Developers
☒ System Administrator
☒ Other

DOI Integrity administrator grants access based on least privilege principle, role-based approach for user account authorization and access enforcement. DOI privilege account holders within the DOI Ethics office are reviewed, authorized and approved by the System Owner.

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

DOI user access to the Integrity system is based on the least privilege principle, role-based approach for user account authorization and access enforcement. DOI privilege account holders supporting Integrity are reviewed, authorized and approved by the DOI Integrity System Owner.

If an employee enters a filing position, they are provided access while they are in that position to complete and view their annual forms. Filer access is restricted to only their own information. Supervisors are provided access based on their supervisory relationship to employees who are filers in order to review filer information and assist in the determination of compliance with applicable Federal conflict of interest laws and regulations. Supervisor access is restricted to only information about filers that they supervise.

DOI Ethics officials are granted access based on their job duties of administering DOI public financial disclosure reports and determining compliance with applicable Federal conflict of interest laws and regulations. DOI Ethics officials at the Department level have access to all DOI information in the system. Ethics officials at DOI bureaus and offices have access restricted to the filers within their organizations.

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

OGE contractors were involved in the design, development and remain involved in the system operation and maintenance. OGE contractors signed Confidentiality and Non-Disclosure Agreements. In addition, OGE's Privacy Act System of Records includes a routine use that allows agencies, including OGE, to disclose information to contractors performing or working on a contract for the Federal Government, when necessary, to accomplish an agency function related to the System of Records Notice.

For DOI, only Federal employees have access to DOI records in Integrity and are system administrators for the DOI use of the Integrity system.

☐ No

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

☐ Yes

☒ No

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

☐ Yes

☒ No

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

Integrity system logs are reviewed on a routine basis to check for unauthorized access or user activity, detect suspicious activity and to support forensic activities to investigate suspected security incidents.

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

DOI is responsible for ensuring DOI user accounts are created and properly managed in accordance with FISMA and NIST guidelines. As the Integrity system owner, OGE is responsible for ensuring adequate controls to prevent unauthorized access or use of the Integrity system. All system usage may be monitored, recorded and is subject to audit.

The DOI Integrity administrator assigns roles for DOI Integrity users based on the principles of least privilege and performs due diligence toward ensuring that separation of duties is in place. DOI is also responsible for providing use and navigation training, including technical and substantive financial disclosure reporting requirements training to support DOI Integrity users. In addition, all users must consent to DOI Rules of Behavior and complete Federal Information System Security Awareness, Privacy and Records Management training, and Privacy Awareness Training before being granted access to any DOI system or information, and annually thereafter.

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

OGE is responsible for ensuring physical controls are implemented and in place to mitigate the privacy risks for unauthorized access. The Integrity servers are located in a secured NITC facility with on-site 24x7x365 security, guard stations, and surveillance and monitoring of building exterior, parking lots and entrances. DOI is responsible for ensuring adequate physical safeguards are in place to protect DOI records in physical locations and preventing unauthorized access to the Integrity system and information.

(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

OGE is responsible for ensuring technical controls are implemented and in place to mitigate the privacy risks for unauthorized access or disclosure of information in Integrity. NITC is FISMA compliant and follows the NIST Risk Management Framework for the selection, implementation and monitoring of security controls to ensure the Integrity system and Federal information are safeguarded. DOI system administrators are responsible for implementing and managing technical controls, managing user accounts and preventing unauthorized access to the system and information.

(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

OGE is responsible for ensuring adequate administrative controls are implemented and in place to mitigate the privacy risks for unauthorized access or disclosure. NITC routinely backs up data and stores it in another Government facility at a different location and the security for those servers and server rooms is comparable to the primary server location. DOI is responsible for ensuring administrative controls are implemented to protect DOI collection, processing and maintenance of records in Integrity, managing user accounts and preventing unauthorized access to the system or information.

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 Designated Agency Ethics Official (DAEO) within the Departmental Ethics Office is the Privacy Act System Manager responsible for ensuring proper collection, maintenance, use and disposal of records in Integrity, addressing Privacy Act requests for access, amendment or complaints, and ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies. The DOI Integrity Information System Owner within the Office of the Solicitor is responsible for working with OGE Integrity officials to perform oversight and management of security and privacy controls to ensure DOI data is securely accessed, processed, stored and disposed of in the Integrity system. These officials are responsible for protecting privacy rights of the public and employees for DOI use of Integrity in consultation with Office of the Secretary Departmental Offices Associate Privacy Officer.

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 DOI Integrity Information System Owner is responsible for the daily operational oversight and management of the Integrity security and privacy controls, for ensuring to

the greatest possible extent that data is properly managed and that access to the data has been granted in a secure and auditable manner. The DOI Integrity Information System Owner, Information System Security Officer, Privacy Act System Manager and the ethics officials within the DOI Ethics Office who are authorized to access the system are responsible for ensuring that any loss, compromise, unauthorized access or disclosure of PII is reported to DOI-CIRC and the Office of the Secretary Departmental Offices Associate Privacy Officer in accordance with Federal policy and established DOI breach response policy and procedures.

OGE and NITC are also responsible for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information as appropriate. OGE is responsible for notifying DOI officials and US-CERT of any incident involving PII and collaborating with DOI representatives to investigate and assess any risk to the Department and individuals. NITC must also follow the incident response and reporting guidance contained in the *FedRAMP* Incident Communications Procedure.