ADAMS ML18134A108

U.S. Nuclear Regulatory Commission

Privacy Impact Assessment

Designed to collect the information necessary to make relevant determinations regarding the applicability of the Privacy Act, the Paperwork Reduction Act information collection requirements, and records management requirements.

Integrity (OGE Application)

Date: May 11, 2018

A. GENERAL SYSTEM INFORMATION

1. Provide a detailed description of the system:

Integrity is a secure, controlled-access, web-based information system created by the U.S. Office of Government Ethics (OGE) for the executive branch of the U.S. Federal Government for electronically filing and reviewing public financial disclosure reports. The system is used to collect, manage, process, and store financial disclosure information from select members of the public in anticipation of nomination by the President and approval by the Senate and certain federal employees. Authorized agency ethics officials use the collected data to identify and resolve potential conflicts of interest between an employee's official duties and his or her private financial interests and affiliations.

OGE developed Integrity in partnership with the Budget Formulation and Execution Line of Business (BFELoB) and the MAX.gov team at the Office of Management and Budget's (OMB) Budget Systems Branch (BSB). Integrity was built using MAX Platform-as-a-Service (MAX PaaS). MAX.gov's FISMA accredited Central Authentication Service (MAX CAS) provides authentication services to the Integrity users (filers and ethics officials).

OGE contracted with the U.S. Department of Agriculture (USDA) National Information Technology Center (NITC) to host Integrity in a secure cloud environment. NITC is a Federal Risk and Authorization Management Program (FedRAMP) authorized cloud service provider. The NITC is Federal Information Security Management Act (FISMA) compliant, following the National Institute of Standards and Technology (NIST) Risk Management Framework for categorization, selection, development, implementation, assessment, authorization, and monitoring of security controls.

2. What agency function does it support?

Integrity is used by applicable NRC employees to file their public financial disclosure reports. The system meets the requirements set forth in the Stop Trading on Congressional Knowledge (STOCK) Act, which was signed into law on April 4, 2012, as amended. Authorized NRC OGC users use the collected information to identify, prevent, and resolve conflicts of interest in accordance with the Ethics in Government Act of 1978 (EIGA). Integrity reduces processing time, eliminates common errors, and improves conflict of interest prevention and resolution.

3. Describe any modules or subsystems, where relevant, and their functions.

Not Applicable

4. What legal authority authorizes the purchase or development of this system?

The Stop Trading on Congressional Knowledge Act of 2012 ("STOCK Act"), Pub. L. No. 112-105, 125 Stat. 191, 298-99 (2012), (as amended); EIGA, 5 U.S.C. app. § 101 et seq as amended, authorizes the use of this system.

5. What is the purpose of the system and the data to be collected?

The purpose of this executive branch-wide system is to electronically collect, manage, process, measure, and store reported financial and related information used in the OGE Form 278 and the OGE Form 278-T. Authorized OGE and NRC users will use the collected information to identify, prevent, and resolve conflicts of interest in accordance with EIGA.

6. Points of Contact:

NRC Integrity Project Manager	**Office/Division/Branch**	**Telephone**
Jay Hosseini	OCIO/ITSDOD/SDMB	301-415-0021
NRC Integrity Administrator	**Office/Division/Branch**	**Telephone**
Rebecca Giitter	OGC/GCLR/LCLSP	301-287-9220
OGE Integrity Project Manager	**Office/Division/Branch**	**Telephone**
George Hancock	OGE	202-482-9309

7. Does this privacy impact assessment (PIA) support a proposed new system or a proposed modification to an existing system?

a. ___ New System ___ Modify Existing System __X__ Other (Explain)

(1) *A PIA for Integrity has not been prepared before. The system is now operational and in use by OGC. No major system changes have occurred. Integrity cybersecurity compliance for the NRC will be managed under the TPS cybersecurity management framework.*

b. If modifying an existing system, has a PIA been prepared before?

(1) If yes, provide the date approved and ADAMS accession number.

(2) If yes, provide a summary of modifications to the existing system.

B. INFORMATION COLLECTED AND MAINTAINED

These questions are intended to define the scope of the information requested as well as the reasons for its collection. Section 1 should be completed only if information is being collected about individuals. Section 2 should be completed for information being collected that is not about individuals.

1. INFORMATION ABOUT INDIVIDUALS

a. Does this system maintain information about individuals?

Yes

(1) If yes, identify the group(s) of individuals (e.g., Federal employees, Federal contractors, licensees, general public).

Covered individuals include members of the public, usually nominees, who are under consideration for Presidentially-appointed, Senate-confirmed (PAS) positions, terminated PAS officials, federal employees who file an OGE Form 278 and/or an OGE Form 278-T, terminated federal employees who file a Termination OGE 278, agency reviewers, and users who administer the system.

(2) IF NO, SKIP TO QUESTION B.2.

b. What information is being maintained in the system about an individual (be specific)?

Any individual who uses the system must provide minimal 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.

c. Is information being collected from the subject individual?

Yes. Individual users are the source of the information.

(1) If yes, what information is being collected?

Any individual who uses the system must provide minimal 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.

d. Will the information be collected from 10 or more individuals who are <u>not</u> Federal employees?

Potentially, yes. Nominees to PAS positions are usually members of the public who will use the system to complete a Nominee OGE Form 278.

(1) If yes, does the information collection have OMB approval?

Yes. OGE developed Integrity in partnership with the Budget Formulation and Execution Line of Business (BFELoB) and the MAX.gov team at OMB's Budget Systems Branch (OMB BSB).

(a) If yes, indicate the OMB approval number:

The OMB control number for Form 278 is 3209-0001 and is referenced in OGE's regulations, at 5 C.F.R. section 2634.601(c).

e. Is the information being collected from existing NRC files, databases, or systems?

No

(1) If yes, identify the files/databases/systems and the information being collected.

N/A

f. Is the information being collected from external sources (any source outside of the NRC)?

Yes. Integrity is used by other Executive Branch agencies, as well as members of the public who have been nominated for PAS positions.

(1) If yes, identify the source and what type of information is being collected?

Any individual who uses the system must provide minimal 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.

g. How will information not collected directly from the subject individual be verified as current, accurate, and complete?

All information about a subject individual will be provided by the subject individual.

h. How will the information be collected (e.g. form, data transfer)?

Not Applicable

2. INFORMATION NOT ABOUT INDIVIDUALS

a. Will information not about individuals be maintained in this system?

Yes.

(1) If yes, identify the type of information (be specific).

Authorized agency users may add necessary related information in accordance with the Ethics in Government Act of 1978 as amended.

b. What is the source of this information? Will it come from internal agency sources and/or external sources? Explain in detail.

The source of this information is authorized Integrity users.

C. USES OF SYSTEM AND INFORMATION

These questions will identify the use of the information and the accuracy of the data being used.

1. Describe all uses made of the data in this system.

Authorized agency ethics officials use the collected data to identify, prevent, and resolve conflicts of interest.

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

Yes. The system collects, manages, processes, renders, and stores public financial disclosure information that responsible officials use to identify, prevent, and resolve conflicts of interest under the Ethics in Government Act of 1978, as amended. The system measures agency processing of its filers' reports.

3. Who will ensure the proper use of the data in this system?

Executive branch agency (NRC) users who have access.

4. Are the data elements described in detail and documented?

Yes

a. If yes, what is the name of the document that contains this information and where is it located?

The data elements are described in the respective information fields that collect the information.

5. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?

No.

a. If yes, how will aggregated data be maintained, filed, and utilized?

b. How will aggregated data be validated for relevance and accuracy?

c. If data are consolidated, what *controls* protect it from unauthorized access, use, or modification?

6. How will data be *retrieved* from the system? Will data be retrieved by an individual's name or personal identifier? (Be specific.)

Yes. The data is retrievable by a filer's name, date, and/or form type (e.g., OGE Form 278, OGE Form 278-T).

7. Will this system provide the capability to identify, locate, and monitor (e.g., track, observe) individuals?

No.

a. If yes, explain.

(1) What controls will be used to prevent unauthorized monitoring?

8. List the report(s) that will be produced from this system.

The system allows authorized users to render the data in an OGE Form 278 or OGE Form 278-T, as applicable.

a. What are the reports used for?

Authorized system users may see management process status reports of the review status of an agency's filers and reports. These reports inform the authorized agency users of the processing status (e.g., assigned, draft, under review or certified) of the agency's filers' reports and other covered documents, measuring completion against standards.

b. Who has access to these reports?

Authorized system users may access these reports. OGE has access to this processing information for all agencies.

D. ACCESS TO DATA

1. Which NRC office(s) will have access to the data in the system?

Only system-registered, authorized users will be granted access to the system. The system will be used by OGC, who will manage accounts and roles for other NRC users who are required to use Integrity to file public financial disclosure reports.

(1) For what purpose?

Authorized NRC users use Integrity to file their public financial disclosure reports as required by the EIGA and STOCK Act.

(2) Will access be limited?

Yes. Access to the system data is role-based. OGC administrators manage accounts and roles for NRC Integrity users.

2. Will other NRC systems share data with or have access to the data in the system?

No.

(1) If yes, identify the system(s).

(2) How will the data be transmitted or disclosed?

3. Will external agencies/organizations/public have access to the data in the system?

Yes.

(1) If yes, who?

Integrity is used by other Executive Branch agencies, as well as members of the public who have been nominated for PAS positions. OGE owns and maintains the system, and has access to system information.

(2) Will access be limited?

Yes. Access to the system data is role-based.

(3) What data will be accessible and for what purpose/use?

Executive branch agency ethics officials and other agency-authorized users have access to the agency's system data for use in determining ethics-related matters, (e.g., conflict of interest of the filer's reported information).

(4) How will the data be transmitted or disclosed?

The data can only be accessed by authorized users when they log into the system.

E. RECORDS RETENTION AND DISPOSAL

The National Archives and Records Administration (NARA), in collaboration with federal agencies, approves whether records are temporary (eligible at some point for destruction/deletion because they no longer have business value) or permanent (eligible at some point to be transferred to the National Archives because of historical or evidential significance). These determinations are made through records retention schedules and are required under 36 CFR 1234.10. The following questions are intended to determine whether the records in the system have an approved records retention schedule or if one will be needed.

1. **Can you map this system to an applicable retention schedule in NUREG-0910, or the General Records Schedules at http://www.archives.gov/records-mgmt/grs ?**

Yes. Data stored in the system is covered by an existing OGE records disposition authority or the General Records Schedules.

a. **If yes, please cite the schedule number, approved disposition, and describe how this is accomplished. For example, will the records or a composite thereof be deleted once they reach their approved retention or exported to a file for transfer based on their approved disposition?**

Employee Ethics Records are covered by GRS 2.8: Employee Ethics Records below:

GRS 2.8: Item 060 – Public financial disclosure reports. Reports for individuals filing and not confirmed by US Senate.

Temporary. Destroy 1 year after nominee ceases to be under consideration for the position or when no longer needed for active investigation, whichever is later**. This disposition is mandatory; deviations are not allowed.**

GRS 2.8: Item 061 – Public financial disclosure reports. All other reports.

Temporary. Destroy 6 years after receipt of OGE Form 278 or 278e by the agency or when no longer needed for active investigations, whichever is later. **This disposition is mandatory; deviations from the instructions are not allowed.**

GRS 2.8 item 062 – Public financial reports. Periodic transaction reports.

Temporary. Destroy 7 years after receipt by the agency of when the related subsequent OGE Form 278 (SF278) is ready for destruction. The reports may be retained longer if needed for active investigation. **This disposition instruction is mandatory; deviations are not allowed.**

If needed, additional scheduling will need to be reviewed according to the following statements below considering the GRS 2.8 states deviations from the above are not allowed:

A filer's data for the OGE Form 278 public financial disclosure reports and related records maintained in the system is identified for deletion from the system in compliance with section 105(e)(2)(d) of EIGA (5 U.S.C. app.): 1 year after the date the individual withdraws or otherwise is no longer under consideration for a Presidentially-

appointed, Senate-confirmed position, or 6 years after the year the report was received for other filers, or when no longer needed for active investigation, whichever is later. Filer's data related to the OGE Form 278-T Periodic Transaction Reports, mandated by the Stop Trading on Congressional Knowledge Act (STOCK Act) of 2012, is to be deleted from the system usually when 7 years old, when the related (subsequent) OGE Form 278 which they support is deleted from the system, or when no longer needed for active investigation, whichever is later.

GRS 3.2 – Item 030 – information Systems Security Records: System access records. Systems not requiring special accountability for access. **Temporary.** Destroy when business use ceases.

Certain information about individuals such as name, executive branch agency, and position title will be deleted manually when all related document data has been deleted. System administration reports will be deleted when OGE determines that they are no longer needed for administrative, legal, audit, or operational purposes under General Records Schedule 3.2, Item 3.

b. If the answer to question E.1 is yes, skip to F.1. If the response is no, complete question E.2 through question E.7.

2. If the records cannot be mapped to an approved records retention schedule, how long do you need the records? Please explain.

3. Would these records be of value to another organization or entity at some point in time? Please explain.

4. How are actions taken on the records? For example, is new data added or updated by replacing older data on a daily, weekly, or monthly basis?

5. What is the event or action that will serve as the trigger for updating, deleting, removing, or replacing information in the system? For example, does the information reside in the system for three years after it is created and then is it deleted?

6. Is any part of the record an output, such as a report, or other data placed in ADAMS or stored in any other location, such as a shared drive or MS SharePoint?

7. Does this system allow for the deletion or removal of records no longer needed and how will that be accomplished?

F. TECHNICAL ACCESS AND SECURITY

1. Describe the security controls used to limit access to the system (e.g., passwords).

Electronic controls, such as password or PIV card authentication, are in place to protect the data. Access to the system is controlled. Access to system information is role-based. Executive branch agencies control their users' access to information. Only users who are registered with credentials at MAX.gov are able to access the system. Detailed information regarding system security controls is documented in the Integrity System Security Plan.

2. What controls will prevent the misuse (e.g., unauthorized browsing) of system data by those having access?

The data view is role-based. Only certain roles have access to filer data. Agencies using the system appoint agency role assignment administrators who assign agency users roles (e.g., filer, reviewer, group administrator) in the system.

3. Are the criteria, procedures, controls, and responsibilities regarding access to the system documented?

Yes.

(1) If yes, where?

Access to the data is role-based. Non-filer users have access depending on their system role(s) as defined in the NRC Integrity SOP. Procedures, controls, and responsibilities regarding access are documented in the Integrity System Security Plan.

4. Will the system be accessed or operated at more than one location (site)?

Yes.

a. If yes, how will consistent use be maintained at all sites?

OGE owns and maintains the Integrity application, and is responsible for securing data on the backend of the system. Other agencies that use the system are responsible for implementing security controls for which they share some or all of the security responsibility, as specified by the Integrity System Security Plan.

5. Which user groups (e.g., system administrators, project managers, etc.) have access to the system?

OGE Integrity system administrators are responsible for the operation and maintenance of the system. NRC has appointed agency role assignment administrators who assign agency user roles (e.g., filer, reviewer, group administrator) in the system.

6. Will a record of their access to the system be captured?

Yes.

a. If yes, what will be collected?

OGC relies on OGE to implement audit logs. Access attempts to the system are captured, including the user attempting access, as well as the date/time of access and whether the access attempt was successful or failed.

7. Will contractors be involved with the design, development, or maintenance of the system?

Yes. Contractors are involved in the design and development of this system. Contractors sign 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.

8. What auditing measures and technical safeguards are in place to prevent misuse of data?

OGC relies on OGE to implement audit logs. Integrity system components, including operating system, database, and application components, generate audit logs. Auditing is configured in accordance with FISMA and NIST requirements.

9. Are the data secured in accordance with FISMA requirements?

Yes.

a. If yes, when was Certification and Accreditation last completed?

The Authorization to Operate (ATO) approval memo was signed by the OGE Authorizing Official on July 28, 2015. An independent security assessment is performed annually.

PRIVACY IMPACT ASSESSMENT REVIEW/APPROVAL
(For Use by OCIO/GEMS/ISB Staff)

System Name: Integrity (OGE Application)

Submitting Office: Office of the General Counsel

A. PRIVACY ACT APPLICABILITY REVIEW

___ Privacy Act is not applicable.

__X__ Privacy Act is applicable.

Comments:

Integrity will be maintained as part of NRC's Privacy Act system of records NRC-4, "Conflict of Interest Files."

Reviewer's Name	Title	Date
Sally A. Hardy	Privacy Officer	6/15/18

B. INFORMATION COLLECTION APPLICABILITY DETERMINATION

___ No OMB clearance is needed.

___ OMB clearance is needed.

__X__ Currently has OMB Clearance. Clearance No. 3209-0001

Comments:

Reviewer's Name	Title	Date
David Cullison	Agency Clearance Officer	5/23/18

C. RECORDS RETENTION AND DISPOSAL SCHEDULE DETERMINATION

___ No record schedule required.

___ Additional information is needed to complete assessment.

___ Needs to be scheduled.

__X__ Existing records retention and disposition schedule covers the system - no modifications needed.

Comments:

Reviewer's Name	Title	Date
Marna B. Dove	Sr. Program Analyst, Electronic Records Manager	5/31/18

D. BRANCH CHIEF REVIEW AND CONCURRENCE

___ This IT system **does not** collect, maintain, or disseminate information in identifiable form from or about members of the public.

__X__ This IT system **does** collect, maintain, or disseminate information in identifiable form from or about members of the public.

I concur in the Privacy Act, Information Collections, and Records Management reviews:

/RA/ Date June 15. 2018

Anna T. McGowan, Chief
Information Services Branch
Governance & Enterprise Management
Services Division
Office of the Chief Information Officer

TRANSMITTAL OF PRIVACY IMPACT ASSESSMENT/
PRIVACY IMPACT ASSESSMENT REVIEW RESULTS

TO: **Office of the General Counsel**	
Name of System: **Integrity (OGE Application)**	
Date ISB received PIA for review: **May 14, 2018**	Date ISB completed PIA review: **June 15, 2018**
Noted Issues:	
Anna T. McGowan, Chief Information Services Branch Governance & Enterprise Management Services Division Office of the Chief Information Officer	Signature/Date: **/RA/ June 15. 2018**
Copies of this PIA will be provided to: *Tom Rich, Director* *IT Services Development & Operation Division* *Office of the Chief Information Officer* *Jonathan Feibus* *Chief Information Security Officer (CISO)* *Governance & Enterprise Management Services Division* *Office of the Chief Information Officer*	