

UNITED STATES OFFICE OF
GOVERNMENT ETHICS



Preventing Conflicts of Interest
in the Executive Branch

Office of Government Ethics
INTEGRITY
Privacy Threshold Analysis (PTA) and
Privacy Impact Assessment (PIA)

INTEGRITY_{gov}
Play your part.

August 13, 2014

U.S. Office of Government Ethics (OGE)
***INTEGRITY* Privacy Threshold Analysis (PTA) and**
Privacy Impact Assessment (PIA)

Name of Project/System: *INTEGRITY*
System ID: OGE-03-MAO-03

Currently under development, *INTEGRITY* will be a secure, controlled-access, web-based information system for the executive branch. It will collect, manage, process, measure, and store financial disclosure information (FDI) 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 will use the collected data to identify, prevent, and resolve conflicts of interest. When deployed executive branch-wide, about 28,000 filers will provide their FDI for review by reviewing officials, such as supervisors and ethics officials.

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). *INTEGRITY* is built using MAX Platform-as-a-Service (MAX PaaS). MAX.gov's Central Authentication Service (MAX CAS) provides authentication services.

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.

Agency representatives will manage their own users and data retention. System data access and information sharing will be role based. The system will eventually replace a paper-based process. A user must be a registered system user and have an authorized/approved role to view system data.

A. CONTACT INFORMATION:

1) Who completed this document?

G. Hancock
eFiling Program Manager
Program Counsel Division
Legal, External Affairs and Performance Branch
Office of Government Ethics
1201 New York Ave, N.W. Suite 500
Washington D.C. 20005-3917
Telephone: 202-482-9309
E-mail: ghancock@oge.gov

2) Who is the system owner?

Diana Veilleux
Chief, Legal, External Affairs and Performance Branch
Program Counsel Division
Office of Government Ethics
1201 New York Ave, N.W. Suite 500
Washington D.C. 20005-3917
Telephone: 202-482-9203
E-mail: diana.veilleux@oge.gov

3) Who is the system manager for this system or application?

G. Hancock
eFiling Program Manager
Program Counsel Division
Legal, External Affairs and Performance Branch
Office of Government Ethics
1201 New York Ave, N.W. Suite 500
Washington, D.C. 20005-3917
Telephone: 202-482-9309
E-mail: ghancock@oge.gov

4) Who is the Chief Information Security Officer who reviewed this document?

Ty Cooper
Chief Information Officer
Office of Government Ethics
Telephone: 202-482-9226
E-mail: ty.cooper@oge.gov

5) Who is the Privacy Officer who reviewed this document?

Diana Veilleux
Privacy Officer
Legal, External Affairs and Performance Branch
Program Counsel Division
Office of Government Ethics
Telephone: 202-482-9203
E-mail: diana.veilleux@oge.gov

6) Who is the Reviewing Official?

Shelley Finlayson
Chief of Staff & Program Counsel
Office of Government Ethics
Telephone: 202-482-9314
E-mail: skfinlay@oge.gov

B. SYSTEM APPLICATION/GENERAL INFORMATION:

1) Does this system contain any information about individuals?

Yes. This system contains information about individuals who submit a public financial disclosure report and their financial information necessary to complete the OGE Form 278 and OGE Form 278-T, as well as digital copies of related ethics information, 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).

Individuals whose information is in the system are nominees to Presidentially-appointed, Senate-confirmed (PAS) positions, terminated PAS officials, federal employees who file the OGE Form 278, Public Financial Disclosure Form, and/or the OGE Form 278-T, Public Financial Disclosure Report: Periodic Transaction Report, and agency users who review filer data or administer the system.

a. Is this information identifiable to the individual?

Yes. When operational, the system will contain information identifiable to the filers completing the online public financial disclosure report. The system requires the filer's name, agency, official position, address, official telephone number, email address, reportable financial information, and other necessary information. Reportable financial information required under the Ethics in Government Act of 1978 (EIGA), 5 U.S.C. app. 101 *et seq* as amended, and implementing regulations may include personal and family holdings (name, amount range, but not account numbers) and 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, non-profit 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. Filers may also optionally provide a personal/home telephone and cell number, a personal email address, and/or a personal, home mailing address. For non-filer users, the system requires the user's name, agency, system role(s)/access permissions, official address, official telephone, and official email address.

b. Is the information about individual members of the public?

Yes. Nominees to PAS positions are usually members of the public who will use the system to complete a Nominee OGE Form 278. In addition, agency users may attach digital copies of related documents, such as ethics agreements, ethics pledge waivers, Certificates of Divestiture, and waivers issued pursuant to 18 U.S.C. §§ 208(b)(1) and (b)(3).

c. Is the information about employees?

Yes. Under the Ethics in Government Act of 1978 (EIGA) as amended, 5 U.S.C. app. §§ 101, 103(l), certain employees of the executive branch are required to file the OGE Form 278 and OGE Form 278-T. Their names, employing agencies, and position titles are in the system. The system also contains data for their OGE Form 278 and OGE Form 278-T, and may contain digital copies of ethics agreements, ethics pledge waivers, Certificates of Divestiture, and waivers issued pursuant to 18 U.S.C. §§ 208(b)(1) and (b)(3).

2) What is the purpose of the system/application?

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 agency users will use the collected information to identify, prevent, and resolve conflicts of interest in accordance with EIGA.

The system implements section 11(b) of the Stop Trading on Congressional Knowledge Act of 2012 (“STOCK Act”), Pub. L. No. 112-105, 125 Stat. 191, 298-99 (2012) (as amended).

3) What legal authority authorizes the purchase or development of this system/application?

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 development of this system.

C. DATA IN THE SYSTEM:

1) What categories of individuals are covered in the system? (E.g., employees, contractors, volunteers, etc.)

Covered individuals include members of the public, usually nominees, who are under consideration for 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) What are the sources of the information in the system?

Users input the information into the system. Filers provide their reportable personal and financial disclosure information. Agency users may add necessary related information in accordance with the Ethics in Government Act of 1978 as amended.

a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?

Individual users are the source of the information.

b. What Federal agencies are providing data for use in the system?

Executive branch agency users add and remove their users (e.g., filers and reviewers) and control access to their filers' information. Executive branch agency users may add information related to reviews of the financial disclosure reports.

c. What State and local agencies are providing data for use in the system?

None.

d. From what other third party sources will data be collected?

None.

e. What information will be collected from the employee and the public?

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.

3) Accuracy, Timeliness, Reliability, and Completeness

a. How will data collected be verified for accuracy?

Individual users are responsible for ensuring the information they enter is accurate and are required to certify to this effect.

b. How will data be checked for completeness?

The system will generate an error message and highlight those that are incomplete required fields.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date?

All data and documents are tagged with the date received and the associated reporting year.

d. Are the data elements described in detail and documented? If yes, what is the name of the document?

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

D. ATTRIBUTES OF THE DATA:

- 1) Is the use of the data both relevant and necessary to the purpose for which the system is being 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.

- 2) Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?**

No.

- 3) Will the new data be placed in the individual's record?**

N/A

- 4) Can the system make determinations about employees/the public that would not be possible without the new data?**

N/A

- 5) How will the new data be verified for relevance and accuracy?**

N/A

- 6) If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?**

Electronic controls, such as password protection, are planned 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.

- 7) If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.**

Electronic controls, such as password protection, are planned to protect access to the data. In addition, access to information in the system is role-based. Executive branch agencies control their users' access to agency information.

- 8) How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.**

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

9) What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

The system allows authorized users to render the data in an OGE Form 278 or OGE Form 278-T, as applicable. Authorized system users may see management process status reports of the review status of an agency's filers and reports. These reports will 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. OGE will have access to this processing information for all agencies.

10) What opportunities do individuals have to decline/refuse to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent.)

Use of the system constitutes a user's consent to sharing their information with authorized users. By using the system, filers consent to the specific uses of their Personally Identifiable Information (PII). The system presents a standard information system use and consent banner at login. The system login page will include this Notice:

WARNING: This is a U.S. Government computer system, use of which is subject to federal law. Unauthorized use of this system is prohibited and may be punishable under the Computer Fraud and Abuse Act of 1986.

INTEGRITY is a U.S. Office of Government Ethics-approved and operated information system. System usage may be monitored, recorded, and subject to audit. Unauthorized use of the system is prohibited and subject to criminal and civil penalties. Use of the system indicates consent to monitoring and recording. By using it and entering your information you acknowledge that authorized users may view your information. Authorized users include your report review chain, assistants you appoint, and system administrative personnel. All such personnel are bound by law, regulation, and policy to safeguard your information from unauthorized access and disclosure. Read the user agreement for more information.

The system will include a link to a user agreement.

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS:

1) If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

The system is hosted in a U.S. Government agency cloud.

2) Is the data in the system covered by existing records disposition authority? If yes, what are the retention periods of data in this system?

Yes, in part. Data to be stored in the system is covered either by an existing OGE records disposition authority or by the General Records Schedules, or by a proposed disposition authority to cover the OGE Form 278-T. The National Archives disposition authority approval is expected in January 2015:

a) 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;

b) 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 20, Items 1 and 4.

3) What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?

The system provides a view of expiring or expired data that has reached its retention duration limit. Authorized system users will use that view to delete the expired information. The retention duration varies: 1 year after an individual withdraws or is no longer under consideration for a Presidentially-appointed, Senate-confirmed position, or 6 years after the year the report was received for individuals who are confirmed by the Senate, or when no longer needed for active investigation, whichever is later; the 278-T Periodic Transaction Reports will be deleted 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. The deletion procedures will be documented in the system user guide.

4) How does the use of this technology affect public/employee privacy?

N/A

5) Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

No.

6) What kinds of information are collected as a function of the monitoring of individuals?

N/A.

7) What controls will be used to prevent unauthorized monitoring?

N/A

8) Under which Privacy Act systems of records notice does the system operate? Provide number and name.

The data collected are covered by the Government-wide, OGE/GOVT-1 Privacy Act System of Records. *See* 68 FR 3098 (January 22, 2003) *as corrected at* 68 FR 24744 (May 8, 2003), *as amended at* 76 FR 24490 (May 2, 2011), 77 FR 45353 (July 31, 2012) and 78 FR 73863 (December 9, 2013).

9) If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.

The OGE Privacy Act System of Records, OGE/GOVT-1, was written to include all information that is necessary for administering provisions of EIGA, the Ethics Reform Act of 1989 and other ethics laws. The system's notice includes all records in the system that are developed or information and material received by the Director of OGE or Designated Agency Ethics Officials in administering the various ethics laws. In addition, the current system of records notice covers records in both paper and electronic form. The OGE Privacy Act System of Records, OGE/GOVT-1, was amended to update the authority for maintaining the system by adding the citation to the STOCK Act, Pub. L. No. 112-105, 126 Stat. 291 (2012) as amended by Pub. L. 113-7 (2013).

10) Other.

A system user's FDI will be encrypted when in transit. A system user's data travels between the user's computer web browser and system servers encrypted by a technology called Secure Sockets Layer (SSL) 256-bit encryption, using Transport Layer Security (TLS) 1.2. The connection is encrypted using an Advanced Encryption Standard (AES), AES_256_CBC, with a Secure Hash Algorithm (SHA), SHA1, for message authentication and RSA as the key exchange mechanism. (SHA1 produces a 160-bit (20-byte) hash value. A SHA-1 hash value is typically rendered as a hexadecimal number, 40 digits long.) RSA is one of the first practicable public-key cryptosystems and is widely used for secure data transmission.

This is the same technology banks use for online transactions, and offers the highest available level of encryption currently supported by web browsers. The lock icon in the

browser window indicates that data is shielded from unauthorized access while in transit. SSL works by using a private key to encrypt data that is transferred over the SSL connection. Many web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, web pages that require an SSL connection start with https: instead of http. Unlike e-filing income tax returns with the Internal Revenue Service, this system does not ask for users' social security numbers, bank account numbers, or investment account numbers, yet the system offers the same security protections.

F. ACCESS TO DATA:

- 1) Who will have access to the data in the system?** (E.g., contractors, users, managers, system administrators, developers, other)

Only system-registered, authorized users will be granted access to the system. System access is password protected. MAX.gov's Central Authentication Service (MAX CAS) provides authentication services. Access to the system data is role-based. Authorized agency users assign roles to other agency users.

- 2) How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?**

Access to the data is role-based. Non-filer users have access depending on their system role(s) as each agency determines.

- 3) Will users have access to all data on the system or will the user's access be restricted? Explain.**

User access to data is restricted based upon their role(s) in the system. For example, an agency user may see status views of filers' reports, but not have permission to see their actual, reported PII.

- 4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of 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.

- 5) Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?**

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

- 6) **Do other systems share data or have access to the data in the system?** If yes, explain.

No, but *INTEGRITY* is connected to MAX.gov's Central Authentication Service for authentication services.

- 7) **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

N/A

- 8) **Will other agencies share data or have access to the data in this system (Federal, State, or Local)?**

Yes. Authorized federal executive branch agency users will see data for filers in their agencies because the system is a federal executive branch-wide enterprise ethics system.

- 9) **How will the data be used by the other agency?**

Executive branch agency ethics officials and other agency-authorized users will 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.

- 10) **Who is responsible for assuring proper use of the data?**

Executive branch agency users who have access.

G. SECURITY OF INFORMATION:

- 1) **Has the system been authorized to process information?**

No. The system is currently under development.

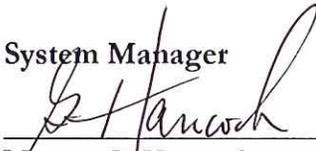
- 2) **Is an annual review of the IT system conducted as required by the Federal Information Security Management Act (FISMA)?**

Once the system is operational, its security controls will be reviewed and tested as required under FISMA.

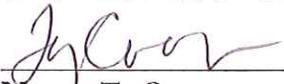
- 3) **Have personnel using the system been trained and made aware of their responsibilities for protecting the PII being collected and maintained?**

Once the system is operational, personnel will be trained and reminded periodically of their responsibilities for safeguarding PII. Annually, users will affirm they are aware of the user agreement and system rules of behavior that include their responsibilities to safeguard PII.

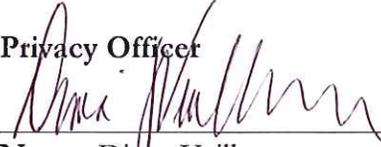
These Officials Have Approved this Document

- 1) **System Manager**


Name: G. Hancock
Title: eFiling Program Manager
(Signature) Aug 13, 2014 (Date)

- 2) **Chief Information Officer**


Name: Ty Cooper
Title: Chief Information Officer
(Signature) Aug 14, 2014 (Date)

- 3) **Privacy Officer**


Name: Diana Veilleux
Title: Privacy Officer
(Signature) Aug 15, 2014 (Date)

- 4) **Reviewing Official**


Name: Shelley Pinlayson
Title: Chief of Staff & Program Counsel
(Signature) Aug 21, 2014 (Date)

Document Revision

The OGE Privacy Officer must approve changes to this document for the changes to be effective.

Date	Page(s)	Description	Author
8/13/14		Initial publication	G. Hancock
8/3/15	Title, p2	Revised to reflect that it is a Privacy Threshold Analysis (PTA) and Privacy Impact Assessment (PIA)	G. Hancock