UNITED STATES

FEDERAL COMMUNICATIONS COMMISSION

PRIVACY IMPACT ASSESSMENT FOR THE OFFICE OF GENERAL COUNSEL BOUNDARY

August 2021

OFFICE OF GENERAL COUNSEL

WASHINGTON, DC 20554

Next Review Cycle: August 2022

Record of Approval

Document Approval		
Drafter Name: Al Shipman		**Bureau/Office: OMD/IR**
SAOP Approval		
Printed Name: Margaret Drake		**Senior Agency Official for Privacy**
Signature: Margaret E Drake Digitally signed by Margaret E Drake DN: cn=Margaret E Drake, o=Federal Communications Commission, ou=Privacy, email=margaret.drake@fcc.gov, c=US Date: 2021.08.03 11:20:29 -04'00'	**Date** 8/3/21	

Record of Approval

Date	Description	Name
07/08/2021	Validation of Information – System Owner	Lauren Northrop
07/20/2021	Validation of completeness – IT Compliance Lead	Liem Nguyen

Revision History

Date	Description	Name
7/29/2021	Original Document Created	ISSO-Al Shipman

Office of General Counsel

1.1. Introduction

Section 208 of the E-Government Act of 2002[1] requires agencies to conduct a **Privacy Impact Assessment (PIA)** whenever they procure or develop an information technology system that will collect, maintain, or disseminate information about individual people. The PIA must document how the system will use information it collects about individuals and, unless it contains classified or sensitive information, it must be made available to the public. The PIA was intended to be a tool for agencies to protect personal information throughout a technology system's life cycle. The Office of Management and Budget (OMB) has commented: "*In general, PIAs are required to be performed and updated as necessary where a system change creates new privacy risks.*"[2]

The FCC is subject to the requirements of the E-Government Act and is committed to identifying and addressing privacy risks whenever it develops or makes changes to its information systems. The questions below explore important privacy issues identified in the Act and in later guidance by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST). A longer discussion of the FCC's PIA policies can be found in Chapter 9 of the FCC's Privacy Act Manual (FCC Inst. 1113.1).

System owners, in collaboration with the Information System Security Officers (ISSOs) should complete the **Initial Privacy Assessment (IPA)** prior to filling out the PIA. The FCC Senior Agency Official for Privacy (SAOP) uses the IPA to determine whether a system will collect the kind of information that would make it subject to the requirements of Section 208, including a PIA. A PIA should not be completed until an IPA is completed and the SAOP makes a determination.

If you have any questions, please contact the Privacy Team at privacy@fcc.gov.

[1] 44 U.S.C. § 3501 note.

[2] OMB Memorandum No. M-03-22 (Sep. 26, 2003), https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2003/m03_22.pdf.

1.2. Authority To Operate (ATO) Boundary Overview

For each IT system that resides within the ATO Boundary, please use the table below to provide the system name, a brief description of the what the system does, whether it contains Personally Identifiable Information (PII) and a brief description of the PII (if applicable), the applicable System of Records Notice, the legal authorities to collect and maintain the PII, and whether the PII is shared with other systems (internal or external).

Please copy the table as necessary to complete the information for each system within the boundary.

INFORMATION ABOUT THE SYSTEM
NAME OF THE SYSTEM Financial Disclosure Online (FDOnline)
DOES THE SYSTEM CONTAIN PII? Yes
PLEASE PROVIDE A BRIEF DESCRIPTION OF THE PII (IF APPLICABLE) Name, salary, and personal financial data as well as work information such as Title, Grade and B/O will be collected. (No DOB, SSN or personal addresses will be in this system).
IN WHAT SYSTEM OF RECORDS (SORN) IS THE INFORMATION CONTAINED (IF APPPLICABLE)? The SORN for the OGE 450 program is OGE/GOVT-2
WHAT ARE THE LEGAL AUTHORITIES FOR THE COLLECTION OF THIS PII? The Ethics In Government Act, 5 USC app. and the regulations found at 5 CFR 2634
DOES THIS SYSTEM SHARE THE PII WITH OTHER SYSTEMS? No

A. Is this a new ATO Boundary or an existing ATO Boundary?

☐ New Boundary

☒ Existing Boundary

B. If the ATO Boundary is/will consist of cloud-based computing system(s),[3] please check the box that best describes the service the FCC receives/will receive from the cloud computing provider:

☒ The FCC uses provider-supported application/s on the provider's cloud network (Software as a Service or SaaS) [list applicable system(s)]

FDOnline is an automated financial reporting system. It is a Software as a Service (SaaS) solution offered by Intelliworx and is used by the FCC to automate the annual financial disclosure process required by Federal employees and other individuals to fulfill their obligations and requirements under the Ethics in Government Act of 1978 and the Ethics Reform Act of 1989, amended, and E.O. 12674 as modified. FDOnline facilitates the automation of the United States Office of Government Ethics (OGE) Form 450 and helps the FCC Ethics Office within the Office of the Solicitor at FCC ensure compliance with Federal conflict of interest laws, and regulation and requirements to preserve and promote the integrity of public officials and institutions.

FDOnline maintains information from year to year so only updates to information are necessary from filers, electronically notifies filers of the annual requirement to file, and guides the filer through the entire form filling process. The application automatically reminds filers of their need to file as due dates approach, allows for electronic filings, and automates management reports on non-filers. FDOnline allows the Ethics Office to review and certify the OGE Form 450 electronically.

☐ The FCC has deployed application/s on the provider's cloud network and the provider supports the applications (Platform as a Service or PaaS) [list applicable system(s)]

☐ The FCC has deployed its own application/s on the cloud network and controls how these application/s are configured and operate (Infrastructure as a Service or IaaS) [list applicable system(s)]

C. **If the IT systems in the ATO Boundary are in the cloud, are the they FedRAMP certified?**

☒ Yes, all the IT systems are FedRAMP certified

[3] *See* NIST, *The NIST Definition of Cloud Computing*, Special Pub. No. 800-145 (Sep. 2011), https://csrc.nist.gov/publications/detail/sp/800-145/final.

☐ No, none, or only some, of the IT systems are FedRAMP certified

Intelliworx / FDOnline became FedRAMP certified in 2018.

1.3. Collection of Data

A. Please explain why it is necessary to collect PII to carry out the purpose of each of the system(s) that maintain PII within this Boundary.

It is necessary to collect PII to carry out the purpose of the system within this Boundary because the data that is required is mandated by the Office of Government Ethics (OGE) and the legal authorities for the collection of this PII. Ethics officials need the supplied PII to review the data in full for any conflicts of interests, concerns, guidance, and compliance that must be disseminated/remediated/enforced.

B. For each system within this Boundary, will this PII be collected from individuals themselves, or from third-parties? If collected from individuals themselves, link to the Privacy Act Statement[4] for each system that is included with the online or paper form the system(s) use(s) to collect the PII.

The PII will be collected from individuals for the most part. The initial input of information from OGC will include Name, Title, Bureau and FCC email address. The employee will add their GS information and/or employment status and will add their personal financial data. Account numbers and monetary values are not required, but the employee could inadvertently include such PII if they mistakenly feel it should be included. The Privacy Act Statement is incorporated in FDOnline as part of the PDF of the OGE Form 450. On each page of the FDOnline filer-side UI, the filer has a link labelled “View PDF” which provides them with a PDF copy of the form they are filling out (with all information added to that point in the process).

C. What steps is the FCC taking to limit the collection of PII to only that which is necessary?

[4] A Privacy Act Statement must inform individuals about (1) the authority to solicit information, (2) the principal purpose(s) for collecting the information, (3) the routine uses for disclosing the information, and (4) whether providing the information is mandatory or voluntary.

OGC Ethics administrators and reviewers specifically check to remove any information that isn't required by OGE, to include PII such as personal and email addresses, monetary values, and account numbers, for example.

What steps will the FCC take to make sure this PII is accurate, complete, and up-to-date?

The user must certify that the information provided on OGE Form 450 is accurate to the best of the filer's knowledge. The annual filing requirement gives the filer an opportunity to update any inaccurate information. FDonline maintains system security log information which includes the username and the action performed.

1.4. Use of the Data

A. Please explain the data flow, including whether the PII will be ingested from, or shared with, another system. Are internal connections reflected in the Cyber Security Asset Management tool (CSAM)? Are Information Sharing Agreements (ISAs) in CSAM for external connections?

The FCC Ethics Program Manager will provide the filer list to the vendor in the form of an excel spreadsheet for initial input. After the initial input, the Ethics Program Manager will maintain the filer list by adding and deleting active filers. The PII is taken from the Employee Roster as provided by OMD/HR as well as provided by the employee/filer.

Authorized FCC employees' access FDOnline via a web application that uses temporary session cookies. Use of the temporary session cookie is necessary to move the user continuously through the system without requiring them to reenter their credentials at each step.

B. Will the information be shared with third-parties as part of the operations of the information system (e.g., through an application programming interface or "API")?

No.

C. How long will the PII be retained and how will it be disposed of?

The data must remain in the system for 6 years as required by the National Archives (NARA) Record Retention guidelines. Once 6 years have passed, the data is expunged by the FDOnline system as required by NARA. The information contained in FDOnline will be disposed of in accordance with NARA GRS 2.8 (Employee Ethics Records).

1.5. Data Security and Privacy

A. What are the system's ratings for confidentiality, integrity, and availability?

Confidentiality	**__High**	**_X__Moderate**	**___Low**
Integrity	**__High**	**_X__Moderate**	**___Low**
Availability	**__High**	**_X__Moderate**	**___Low**

B. Discuss the physical, administrative, and technical controls in place to protect the data in the system.

In addition to the controls provided in the FedRAMP baseline, the FCC protects its information resources with a dynamic set of security measures. Some of these measures (e.g., network firewalls, physical security) protect the entire FCC enterprise, while other measures (e.g., user access restrictions, encryption) are applied to specific information systems. Following the risk-based policy established in the Federal Information Modernization Act (FISMA), the FCC applies more security measures (also known as security "controls") to information systems that present higher operational risks. Consistent with this policy, the FCC applies specific security controls to systems that collect and process PII. A comprehensive list of the security and privacy controls the FCC may apply to its information systems can be found in National Institute of Standards and Technology (NIST) Special Publication No. 800-53 (revision 4), ttps://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final.

C. Does the system inherit privacy controls from an external provider? If an Interconnection Security Agreement (ISA) , Memorandum of Understanding (MOU) , or similar document is in place, please summarize the privacy applicable portions of the document.

FDOnline does not inherit privacy controls from an external provider.

1.6. Access to the Information

A. Which FCC employees and contractors will have access to the PII in this information system?

The OGC Ethics Team will have access to all documents in FDonline.

B. Does this system leverage Enterprise Access Controls?

Yes

C. Does the system leverage the FCC's Accounting for Disclosure control?

Yes. The Privacy Team keeps an accurate accounting of disclosures of information.