Template Version Number: 01-2020

U.S. Department of Commerce
Office of General Counsel

Privacy Threshold Analysis
for the
Intelliworx Cloud V.9
FDOnline Application Module Service

U.S. Department of Commerce Privacy Threshold Analysis

Office of General Counsel /Intelliworx FDOnline Module

Unique Project Identifier: FR1724526654

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a general description (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

The Intelliworx Cloud platform is a software application platform that allows customer agencies to streamline and automate workflows in any number of mission areas.
Software modules built on the Intelliworx Cloud platform allows users to:

- Define the people who are part of a given business workflow: assigning them roles, permissions, tasks, and responsibilities.
- Gather information critical to the workflow in a streamlined and intuitive way.
- Define the tasks that need to be completed by users and provide mechanisms for approvals, notifications/reminders, and reporting.
- Integrate with existing government systems to accept, process and store data.
- Map gathered data to official government forms.

The Intelliworx platform is also a suite of tools that allows customized solutions called *modules*.
At the code level, the Intelliworx platform is a common set of code libraries that allow for the creation of software "modules" that perform specific process automation functions based upon customer requirements.
At an application level, Intelliworx modules appear as independent web applications with unique URLs and separate logins for each web application. Customers are given access to only the URL and login appropriate for the module(s) they are using.

At the infrastructure level, the Intelliworx Cloud is an environment hosted and secured at AWS GovCloud. Multiple Intelliworx modules are hosted in this environment but are completely segregated except when an integration is authorized between two modules. The only services shared by these modules are the security systems that oversee them.

Through review and analysis, it has been determined that the baseline security categorization for the system is listed in the Table-1. Baseline Security Configuration that follows.

Table-1. Baseline Security Configuration

Intelliworx FIPS-199 Security Categorization	Moderate (M)

(a) *Whether it is a general support system, major application, or other type of system*
Intelliworx FDOnline Module is layer considered application portal which is part of a Major FedRamp approved Cloud Service.

(b) *System location*
Intelliworx FDOnline Module is accessed through a web portal. System access and accounts are ma intained through a designated representative out of the OGC Ethics office for account access. The System(s) that support the Intelliworx various modules are located in the Intelliworx Cloud V.9 which is supported by AWS Government Cloud Services located in the Data Center, Ashburn, Virginia.

(c) *Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*
Intelliworx FDOnline Module is a standalone module that interconnects with the larger Intelliworx Cloud V.9 Services supported by AWS Government Cloud Services and does not share any connectivity with other systems nor does its cross reference with any other resources utilized by OGC or Department of Commerce offices.

(d) *The purpose that the system is designed to serve*
The Intelliworx platform is a software application platform that allows customer agencies to streamline and automate workflows in any number of mission areas. For the OGC office the module being utilized is the Financial Disclosure module which is a workflow designed to efficiently emulate the Office of Government Ethics (OGE) filing process mandated for federal employees. This system covers the OGE- 450 filing types as well as other, supplemental, forms that may be required.

(e) *The way the system operates to achieve the purpose*
Intelliworx FDOnline Module information is retrieved by the end user through a portal connectivity with assigned User access. OGC will use this technology at the application level. Intelliworx modules appear as independent web applications with unique URLs and separate logins for each web application. Customers are given access to only the URL and login appropriate for the module(s) they are using.

(f) *A general description of the type of information collected, maintained, used, or disseminated by the system*
The OGC staff and support will be utilizing this application as a safe and secure way to file their confidential financial disclosures. The type of financial data collected is a range from income, assets, debts to expenses of a federal employee. The new application service will allow all disclosure forms to be tracked and accessed by teleworking employees and ensure the forms are efficiently and effectively reviewed.

(g) *Identify individuals who have access to information on the system*
Customer Application Administrators-Responsible for Support and manage the application for their appointed organization only. The initial customer application administrator can create additional administrators with full or restricted access to various rights within their organization. Customer application administrators never have access to rights, data, or configurations that are server-wide

or belong to other customers. Intelliworx Application Administrators-Responsible for support and manage the application. Create users, objects, modify workflows, modify configurations, and perform troubleshooting. Intelliworx Application Administrators have access to all data. Intelliworx Users will have full access to their own data and even after it has been archived.

(h) How information in the system is retrieved by the user

Intelliworx FDOnline Module information is retrieved by the end user through a secured portal connectivity with assigned User access.

(i) How information is transmitted to and from the system

A user using the application enters the URL which is resolved through our DynDNS managed DNS service to one of three public IPs. Each public IP is attached to a Palo Alto firewall (in FIPS mode) which performs inbound SSL traffic inspection, malware scanning, behavior analysis, and other security activities. Only HTTPS traffic is allowed in. HTTPs servers change and obscure the URL and port and pass the user off to AWS GovCloud Elastic Load Balancers (ELB) associated with the module they are accessing.

Questionnaire:

1. Status of the Information System

1a. What is the status of this information system?

_x_ This is a new information system. *Continue to answer questions and complete certification.*

____ This is an existing information system with changes that create new privacy risks.
Complete chart below, continue to answer questions, and complete certification.

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or 01-2017). *Continue to answer questions and complete certification.*

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2019 or later). *Skip questions and complete certification*

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

x Yes. This is a new information system.

____ Yes. This is an existing information system for which an amended contract is needed.

____ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

____ No. This is not a new information system.

2. Is the IT system or its information used to support any activity which may raise privacy concerns?
NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____ Yes. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

x No.

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?
As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

x Yes, the IT system collects, maintains, or disseminates BII.

____ No, this IT system does not collect any BII.

4. Personally, Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

__x__ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

- __x__ DOC employees
- ___ Contractors working on behalf of DOC
- __x__ Other Federal Government personnel
- ___ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

____ Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.
Provide the legal authority which permits the collection of SSNs, including truncated form.

__x__ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

__x__ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

_____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

__x__ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the SAOP approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X__ I certify the criteria implied by one or more of the questions above **apply** to the Intelliworx FDOnline Module and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the Intelliworx FDOnline Module and because of this non-applicability, a PIA for this IT system is not necessary.

Information System Security Officer or System Owner Name: David Maggi Office: Office of General Council / OGX Phone: 202.482.7938 Email: dmaggi@doc.gov Signature: DAVID MAGGI Digitally signed by DAVID MAGGI Date: 2021.02.24 11:15:18 -05'00' Date signed:	**Information Technology Security Officer** Name: Jerome Nash Office: Office of the Chief Information Officer Phone: 202.482.5929 Email: jnash@doc.gov Signature: JEROME NASH Digitally signed by JEROME NASH Date: 2021.02.25 13:11:19 -05'00' Date signed:
Privacy Act Officer Name: Tahira Murphy Office: OPOG Phone: 202.482.8075 Email: Tmurphy2@doc.gov Signature: Tahira Murphy Digitally signed by Tahira Murphy Date: 2021.03.03 12:12:48 -05'00' Date signed:	**Authorizing Official** Name: Lawrence W. Anderson Office: Office of the Chief Information Officer Phone: 202.482.2626 Email: landerson@doc.gov Signature: LAWRENCE ANDERSON Digitally signed by LAWRENCE ANDERSON Date: 2021.02.26 14:39:21 -05'00' Date signed:
Bureau Chief Privacy Officer Name: Maria Dumas Office: Office of the Privacy and Open Government Phone: 202.482.5153 Email: mdumas@doc.gov Signature: MARIA STANTON-DUMAS Digitally signed by MARIA STANTON-DUMAS Date: 2021.03.03 13:20:49 -05'00' Date signed:	