Template Version Number: 01-2021

U.S. Department of Commerce
Office of the Secretary

Privacy Impact Assessment
for the
Intelliworx Cloud V.9
FDOnline Application Module Service

Reviewed by: Maria D. Dumas, Bureau Chief Privacy Officer

☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Jennifer Goode 2/28/2022

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
Office of the Secretary/Intelliworx FDOnline Module

Unique Project Identifier: FR1724526654

Introduction: System Description

Provide a brief description of the information system.

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 as listed in the Table-1. Baseline Security Configuration that follows: Intelliworx FIPS-199 Security Categorization – Moderate (M).

Address the following elements:

(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 not supported in Department of Commerce spaces but is accessed through a web portal. System access and accounts are maintained 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 way the system operates to achieve the purpose(s) identified in Section 4*
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.

(e) *How information in the system is retrieved by the user*
Intelliworx FDOnline Module information is retrieved by the end user through a portal connectivity with assigned user access.

(f) *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 assessing.

(g) *Any information sharing*
There is no information sharing between Systems or Modules. Each Module is identified based on customer customization.

(h) *The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information*
The specific programmatic authorities for collecting, maintaining, using, and disseminating the information are covered under the Paperwork Reduction Act for submission to Ethic's forms OMB# 3209-0006 OGE form 450.

(i) *The Federal Information Processing Standards (FIPS) 199 security impact category for the system*
The Federal Information Processing Standards (FIPS) 199 security impact category for the system has been determined through FedRAMP as Moderate.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

_____ This is a new information system.
_____ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

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.

__X__ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		f. Driver's License		j. Financial Account	X
b. Taxpayer ID		g. Passport		k. Financial Transaction	
c. Employer ID	X	h. Alien Registration		l. Vehicle Identifier	
d. Employee ID	X	i. Credit Card		m. Medical Record	
e. File/Case ID					
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	X	h. Date of Birth	X	o. Financial Information	
b. Maiden Name	X	i. Place of Birth		p. Medical Information	
c. Alias	X	j. Home Address	X	q. Military Service	
d. Gender		k. Telephone Number		r. Criminal Record	

e. Age		l. Email Address	X	s. Marital Status	
f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X	e. Work Email Address	X	i. Business Associates	
b. Job Title	X	f. Salary	X	j. Proprietary or Business Information	
c. Work Address	X	g. Work History		k. Procurement/contracting records	
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information			
l. Other work-related data (specify): Grade					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		f. Scars, Marks, Tattoos		k. Signatures	
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording		h. Eye Color		m. DNA Sample or Profile	
d. Video Recording		i. Height		n. Retina/Iris Scans	
e. Photographs		j. Weight		o. Dental Profile	
p. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	X
b. IP Address	X	f. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person		Hard Copy: Mail/Fax		Online	X
Telephone		Email			
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify):					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Describe how the accuracy of the information in the system is ensured.

The information in the system is provided by the employee/filer. Therefore, the accuracy lies within the individual input, as it did with the paper filing system.

2.4 Is the information covered by the Paperwork Reduction Act?

X	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. **OMB# 3209-0006 OGE form 450**
	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

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

X	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online	X	For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify):			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

This information is collected as required for review and submission of individual employee's Office of Government Ethics (OGE) Form 450. The DOC Ethics Office collects and reviews the OGE form 450 as has been the practice with the paper filing system. The financial data collected is only used and seen internally by DOC. The information provided is used by DOC Ethics to avoid filer involvement in a real or apparent conflict of interest. The purpose of the form is to assist employees and their agencies in avoiding conflicts between official duties and private financial interests or affiliations.

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

One potential threat is insider threat because of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled. For example, Cyber Security Awareness and Insider Threat training is offered through OGC and DOC training guidelines. Additionally, from a technical aspect, the modules are set up as a Role Based Access System. (i.e., System Administrator Roles, Client Services Roles and User Roles). All of which are monitored though SIEM tools and logging mechanisms. There are no other potential threats to privacy, as system only logs individual filer reported information. Penalty warnings are listed within the system are describe as shown below: Falsification of information or failure to file or report information required to be reported may subject the filer to disciplinary action by their employing agency or other authority. Knowing and willful falsification of information required to be reported may also subject the filer to criminal prosecution.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau			X
DOC bureaus			
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

	The PII/BII in the system will not be shared.

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
X	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
X	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.4 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

Personal Roles and Privileges

Role	Internal or External	Privileged (P), Non-Privileged (NP), or No Logical Access (NLA)	Sensitivity Level	**Authorized Privileges**	Functions Performed

Intelliworx Infrastructure Administrators	Internal	P	Moderate	**Full Infrastructure Access** **Limited Application Access** **No Security Systems Access**	Support and manage (create, remove, modify, modify access to, update, patch) all infrastructure systems: AWS GovCloud, Linux servers, MySQL databases, Tomcat, HTTP, Splunk, and Palo Alto firewalls. Maintain an account in the application for the administration and support of server wide functions in the application (scheduling jobs, troubleshooting email notifications, etc.).
Intelliworx Security Administrators	Internal	P	Moderate	**Limited Infrastructure Access** **No Application Access** **Full Security Systems Access**	Operate, support, and manage (create, remove, modify, modify access to, update) all security systems as needed. Perform vulnerability and compliance activities, review system integrity checks and malicious code monitoring. In the case of a security investigation, security administrators may be given heightened access to all infrastructure systems and applications.
Intelliworx Application Administrators	Internal	P	Moderate	**No Infrastructure Access** **Full Application Access** **No Security Systems Access**	Support and manage the application. Create users, objects, modify workflows, modify configurations, and perform troubleshooting. Intelliworx Application Administrators have access to all data.

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: https://fd- uat.intelliworxit.com/client/auth/login.view and on OGE Form 450.	
X	Yes, notice is provided by other means.	Specify how: Privacy Act Notice is presented to account users, see **Attachments A and B.**
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
X	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: PII is required to complete Office of Government Ethics (OGE) Form 450.

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: Intelliworx individuals are provided access to the Intelliworx system in accordance with established account provisioning and management processes that take into account their roles and responsibilities.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Prior to finalizing their OGE form 450 submission they can update change or review. Filers within the Intelliworx: FD (FDOnline) module are required to update their PII on an annual basis when reporting their financial assets. Individual filers can

		work with the agency's designated ethics administrator to request access to their records and reopen a filing if PII needs to be updated for the current filing year.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

X	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: All login activities to the Intelliworx system are logged. Additionally, infrastructure logs related to privileged functions, administrator activity, and data changes and deletions are automatically input into the Splunk Security Information and Event Management (SIEM) tool for automated monitoring and analysis to detect suspicious activity and indicators of inappropriate or unusual activity. Application security logs are available for review by Intelliworx Security Officers via SQL from the database.
X	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): ___01/24/2022_____ ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
X	Contracts with customers establish DOC ownership rights over data including PII/BII.
X	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

Implementation of the NIST 800-53 Rev 4 controls for a FedRAMP Moderate system (e.g., access controls, encryption, border protection, security monitoring, security awareness training). All modules are located within the Amazon Web Services (AWS) GovCloud Infrastructure, Intelliworx Cloud Service (SaaS) Major Application and is accessed through various modules as a (IaaS) Service.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

_X__ Yes, the PII/BII is searchable by a personal identifier.

____ No, the PII/BII is not searchable by a personal identifier.

9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: • COMMERCE/DEPT-18 – Employees Personnel Files Not Covered by Notices of Other Agencies • COMMERCE/DEPT-25 - Access Control and Identity Management System
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: Ethics in Government Act of 1978
	No, there is not an approved record control schedule.

	Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding		Overwriting	
Degaussing		Deleting	X
Other (specify): This is an online system. All data will be deleted IAW DOC data storage and disposal policy. Once data has reached the six (6) year maximum retention period within FDOnline, records are moved to a queue where customers (e.g., data owners) must designate whether the record can be purged or if the record needs to be held The Intelliworx system does not maintain reports that contain PII as there is no need or business process that necessitates this.			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
X	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact level. *(Check all that apply.)*

X	Identifiability	Provide explanation: All login activities to the Intelliworx system are logged. Additionally, individuals are identified by employer ID and Employee ID.
X	Quantity of PII	Provide explanation: Only the individual whose information the forms pertain to has access along with the authorized reviewer. OGC Ethics department determines what is required to complete the necessary information for OMB# 3209-0006 OGE forms.
X	Data Field Sensitivity	Provide explanation: All personnel have their status categorized with a sensitivity level in accordance with NIST Control PS-2. Employees of the service are considered Internal Users and are

		only given specific permission to perform specific function as it pertains to their Data upload.
X	Context of Use	Provide explanation: Only data pertinent to that that individuals filing is maintained, used and dissemination is limited to only personnel authorized to review.
X	Obligation to Protect Confidentiality	Provide explanation: IAW the Privacy Act of 1974, NIST 800-53rev4, NIST Special Publication 800-122, NIST SP 800-145. The confidentiality of the individual's data is carefully monitored and maintained and access to the data is only by that individual or personnel authorized to review.
X	Access to and Location of PII	Provide explanation: The Intelliworx Cloud V.9 system operates within and leverages the Amazon Web Service (AWS) GovCloud Infrastructure as a Service (IaaS) environment. Intelliworx utilizes the AWS GovCloud IaaS multiple security measures.
X	Other:	Provide explanation: FedRAMP package approved at the moderate level FR1724526654.

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

Intelliworx has identified and evaluated any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. At the user level, Insider Threat considerations and mechanisms have been put into place to identify individual's identity and validation of the data. There are no potential threats. The Intelliworx Cloud V.9 system operates within and leverages the AWS GovCloud Infrastructure as a Service (IaaS) environment. Cyber Security Awareness and Insider Threat training is offered through OGC and DOC training guidelines. Additionally, from a technical aspect, the modules are set up as a Role Based Access System. (i.e., System Administrator Roles, Client Services Roles and User Roles).

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

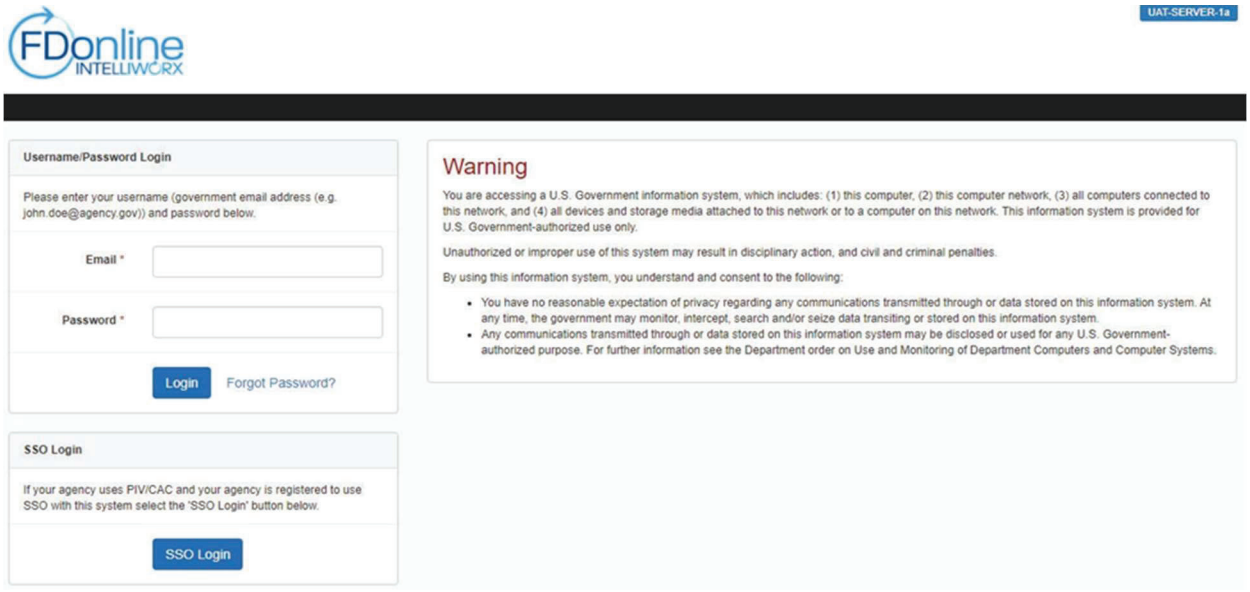
X	Yes, the conduct of this PIA results in required business process changes. Explanation: The OGC ethics office no longer collects the OGE 450 paper filings as this system has replace the paper filing system previously used.

	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.

Attachment A



Attachment B