FedRAMP
Privacy Impact Assessment

Intelliworx

Intelliworx Cloud

Version 9.1

November 22, 2019

Prepared by

SecureIT		
SECURE IT	Street Address	1818 Library Street
	Suite/Room/Building	Suite 500
	City, State, ZIP	Reston, VA 20190

Prepared for

Intelliworx		
INTELLIWORX	Street Address	21400 Ridgetop Circle
	Suite/Room/Building	Suite 210
	City, State, ZIP	Sterling, VA 20166

Record of Changes

Date	Description
9/30/2016	Sec 1.2 clarity rewrites; and added Voice recordings to list of PII examples Sec 2 clarity rewrites; Sec 3.1-3. Added NIST control identifiers and edits to questions Removed Acronyms and referenced FedRAMP Master Acronyms and Glossary resource document

Revision History

Detail specific changes in the table below.

Date	Version	Description	Author
8/7/2017	1.0	Initial Version	SecureIT
6/20/2018	1.1	Review for effectiveness	Laurence Kirby
7/24/2018	1.2	Boundary review	Laurence Kirby
2/11/2019	9	2019 review and version numbering change	Mike Howlett
11/21/2019	9.1	Revised original specifically for FERC	Laurence Kirby

How to contact us

For questions about FedRAMP, or for technical questions about this document including how to use it, contact *info@fedramp.gov.*

For more information about the FedRAMP project, see www.fedramp.gov.

Table of Contents

List of Tables

1 PRIVACY OVERVIEW AND POINT OF CONTACT (POC)

The Table 1-1 – Intelliworx Privacy POC individual is identified as the Intelliworx Privacy Officer and POC for privacy at Intelliworx.

Table 1-1 – Intelliworx Privacy POC

Name	Laurence Kirby
Title	Privacy Officer
CSP / Organization	Intelliworx
Address	21400 Ridgetop Circle, Sterling, VA 20166
Phone Number	703-260-6339
Email Address	Laurence.kirby@intelliworxit.com

1.1 APPLICABLE LAWS AND REGULATIONS

The FedRAMP Laws and Regulations can be found on: www.fedramp.gov.

Table 1-2 Intelliworx Laws and Regulations include additional laws and regulations specific to Intelliworx. These will include laws and regulations from the Federal Information Security Management Act (FISMA), Office of Management and Budget (OMB) circulars, Public Law (PL), United States Code (USC), and Homeland Security Presidential Directives (HSPD). All applicable Laws and Regulations are referenced in Attachment Intelliworx A12 Laws and Regulations v1.0 located on MAX.gov.

Table 1-2 Intelliworx Laws and Regulations

Identification Number	Title	Date	Link
N/A	N/A	N/A	N/A

1.2 PERSONALLY IDENTIFIABLE INFORMATION (PII)

Personally Identifiable Information (PII) as defined in OMB Memorandum M-17-12 refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Information that could be tied to more than one person (e.g., date of birth) is not considered PII unless it is made available with other types of information that together could render both values as PII (for example, date of birth and street address). A non-exhaustive list of examples of types of PII includes:

- Social security numbers
- Passport numbers
- Driver's license numbers

- Biometric information
- DNA information
- Bank account numbers
- Voice recordings

PII refers to information that can be traced back to an individual person.

2 PRIVACY DESIGNATION

Cloud Service Providers (CSPs) perform an annual analysis to determine if PII is collected by any of the system components. Clouds that do not collect PII and would like to opt out of hosting privacy information may elect to do so and are not required to fill out the Privacy Impact Assessment (PIA) Questions. If a CSP is willing to host PII, the Privacy Impact Assessment Questions should be answered given the current knowledge of the CSP. A CSP is not required to solicit customers for the information.

Federal cloud customers (i.e., data owner/system owners) are required to perform their own PIAs and may share this information with the CSP if they so desire (for informational purposes and/or to work with the CSP to develop processes and procedures for managing their PII).

Threshold Analysis

Check one.

☐ Opt out. This cloud will not host privacy information.
☒ This cloud is willing to host privacy information.

Select the cloud layers that are represented by the Intelliworx system. Select all that apply.

☒ This cloud includes Software as a Service (SaaS).
☐ This cloud includes Platform as a Service (PaaS).
☐ This cloud includes Infrastructure as a Service (IaaS).

3 PRIVACY IMPACT ASSESSMENT TALKING POINTS

According to NIST SP 800-122, Appendix D,

> There must be no personal data record-keeping systems whose very existence is secret.

Additionally, NIST SP 800-122, Appendix D states,

> There should be a general policy of openness about developments, practices, and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data and the main purposes of their use, as well as the identity and usual residence of the data controller.

In light of the NIST guidance, PIA talking points have been developed for the purpose of ensuring full disclosure between stakeholders.

Identifiers in parenthesis after a section title indicate NIST SP 800-53, Appendix J privacy controls that are related to the particular talking point. These mappings to Appendix J privacy controls are not considered a replacement for Appendix J controls.

3.1 PII MAPPING OF COMPONENTS (SE-1, DM-1)

General Service (GS) Supervisory employees (i.e., GS15s, GS14s, and GS13s) are required by the Office of Government Ethics (OGE) regulation to submit a Confidential Financial Disclosure Report, OGE Form 450, annually. Employees will be able to electronically file Form 450 using the Financial Disclosure (FD)online, a financial disclosure filing system.

The FDonline module is a cloud-based, multi-tenant, software as a service (SaaS) - that sits on the Intelliworx platform - which allows applicable government employees and ethics officers to efile and review the annual OGE Form 450. The Intelliworx platform allows customer agencies to streamline and automate workflows in any number of mission areas. The platform consists of modules. The module discussed in this PIA is FDonline. Each module has been analyzed to determine if any elements of that module collect and/or store PII. The type of PII collected and/or stored by Intelliworx and the functions that collect it are recorded in Table 3-1.

Table 3-1 PII Mapped to Modules

Modules	Does this Component Collect or Store PII? (Yes/No)	Type of PII	Reason for Collection of PII	Safeguards
(FDonline)	Yes	Federal employee full name, employment information, financial information (e.g., assets, income and valuation of assets) for self and spouse/family	Required to submit OGE Form 450	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 as a Service (IaaS).

3.2 PROSPECTIVE PII USE

Respond to the following questions:

1. Are there any data fields in the platform or application that have been targeted for the collection or storage of PII? If yes, please name those fields. (SE-1, DM-1, IP-1)

Yes. The Intelliworx system (FDonline module) collects the following PII for the inherent purposes of onboarding new hires and filing financial disclosure forms:

- Full name
- Email address
- Demographics (e.g., race, nationality, ethnicity)
- Employment: work address, e-mail address grade, title, work phone
- Types and amounts of salaries, investments, and assets for self and spouse/family
- Creditor names, city, state, country

2. If PII fields are used, can individuals "opt-out" of PII fields by declining to provide PII or by consenting only to a particular use (e.g., allowing basic use of their personal information, but not sharing with other government agencies)? (IP-1)

Within the FDonline module, individuals are not able to opt out of providing PII or consenting to only a particular use. The PII collected and used is required by the OGE. Declining to provide PII effectively declines employment.

☐	Yes	Explain the circumstances of being able to opt-out of PII fields (either for specific data elements or specific uses of the data). (IP-1) .
☒	No	It is not possible to opt-out. PII will be used only for the purpose for which it is collected.

3.3 SOURCES OF PII AND PURPOSE

3. Does Intelliworx have knowledge of existing federal agencies that provide PII that gets imported into the system? (AP-2)

Yes, federal agencies that are customers and users of the Intelliworx system (FDonline module) provide PII as input to the system.

4. Has any agency that is known to provide PII to the system provided a stated purpose for populating the system with PII? (AP-1, AP-2)

Not explicitly. However, federal agency customers populating the system (through FDonline) with PII is integral to the business processes of the Intelliworx system.

5. Does Intelliworx currently populate the system with PII? If yes, where does the PII come from and what is the purpose? (AP-1, AP-2)

Intelliworx only populates the Intelliworx system with PII during the initial onboarding of customers if the federal agency provides the data to be loaded into the system.

The FDonline module can be populated by flat files provided by FERC. However, FERC employees will complete OGE 450 form electronically by accessing FDonline.

The collection of PII is integral to the business processes of the Intelliworx system.

6. Will any third party sources be providing PII that will be imported into the system (if known)? Please explain. (AP-1, AP-2)

The individual who is onboarding to FERC and completing the OGE 450 form provides PII to be imported into the Intelliworx system.

3.4 ACCESS TO PII AND SHARING

7. What third-party organizations will have access to the PII (if known)? Who establishes the criteria for what PII can be shared? (AP-1, AP-2, AR-8, IP-1, UL-2)

The FDonline module does not provide PII to any third-party organizations.

FERC establishes the criteria for granting system account access to the PII managed by Intelliworx.

8. What Intelliworx personnel roles will have access to PII fields (e.g., users, managers, system administrators, developers, contractors, other)? Explain the need for Intelliworx personnel to have access to the PII. (AR-8, UL-2)

Intelliworx utilizes a role-based approach for Intelliworx system account management activities. Access to the Intelliworx system, and the PII fields contained within, is limited to Intelliworx personnel with an application, infrastructure, or security administrator role supporting the Intelliworx system. Individuals are only granted access to functionality necessary to accomplish assigned tasks and responsibilities, such as application support and system administration.

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 (e.g., create, remove, modify, modify access to, update, patch) all infrastructure systems: Amazon Web Services (AWS) GovCloud, Linux servers, MySQL (Structured Query Language) databases, Tomcat, Hypertext Transfer Protocol daemon (HTTPd), Splunk, RADIUS, and Palo Alto firewalls. Maintain an account in the application for the administration and support of server-wide functions in the application (e.g., scheduling jobs, troubleshooting email notifications).
Intelliworx Security Administrators	Internal	P	Moderate	**Limited Infrastructure Access** **No Application Access** **Full Security Systems Access**	Operate, support, and manage (e.g., 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.

9. For Intelliworx support staff, how is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access to PII require manager approval? (IP-2)

Intelliworx personnel are granted access to the Intelliworx system based on role, and only have access to functionality that is necessary to accomplish assigned tasks and responsibilities, such as application support and system administration. Access and authorization requests are documented, authorized, and approved by the individual's manager and the Intelliworx Security Officer prior to account creation.

10. Do other systems that interconnect to the system share, transmit, or access the PII in the system? If yes, explain the purpose for system to system transmission, access, or sharing of PII. (UL-2)

No. Other systems do not share, transmit, or access the PII in the system.

3.5 PII SAFEGUARDS AND LIABILITIES

11. What controls are in place to prevent the misuse (e.g., browsing) of PII by those having access? (AR-2)

Intelliworx individuals are provided access to the Intelliworx system in accordance with established account provisioning and management processes that take into account personnel screening requirements from the agency. Additionally, Intelliworx provides security awareness training to all employees and displays a warning banner each time an individual logs onto the system, describing that unauthorized or improper use may result in disciplinary action and civil and criminal penalties.

12. Who will be responsible for protecting the privacy rights of the individuals whose PII is collected, maintained, or shared on the system? Have policies and/or procedures been established for this responsibility and accountability? (AR-1, AR-2)

The Intelliworx Privacy Officer is responsible for protecting the privacy rights of the individuals whose PII is within the Intelliworx system. Prior to being granted system access, Intelliworx requires that internal users acknowledge the Intelliworx Rules of Behavior, including the requirements for protection of information. As part of the Intelliworx customer onboarding process, the federal agency customer administrator must acknowledge the Intelliworx Rules of Behavior, including the reference to the Privacy Act and requirements for protection of information.

Each agency's Privacy Officer is accountable for the data owned by the agency and for making Intelliworx aware of the agency's policies regarding the collection, maintenance, and sharing of PII. The agencies are responsible for the data that they extract from the system and for following their own privacy policies and procedures.

13. Does Intelliworx provide annual security training include privacy training? Does Intelliworx require their contractors that have access to the PII to take the training? (AR-5)

Yes. Intelliworx includes privacy training as part of the annual security awareness training provided to Intelliworx support personnel.

Intelliworx does not have contractors supporting the Intelliworx system.

All contractor employees and subcontractor employees requiring access to FERC information and information systems will be required to sign and acknowledge FERC Rules of Behavior relating to access to FERC information and information systems, complete FERC Cyber Security Awareness Training (CSAT) and annual refresher training as required, complete FERC general privacy training and annual refresher training as required, complete any additional cyber security or privacy training (e.g., role-based information security, Information Technology Security Training requirements), and build an Information Technology Security Awareness and Training program.

14. Who is the privacy officer responsible for assuring safeguards for the PII? (AR-1)

Laurence Kirby maintains the role of Privacy Officer and is responsible for assuring safeguards for the PII within the Intelliworx system.

15. What is the magnitude of harm to the individuals if privacy related data is disclosed, intentionally or unintentionally? (AR-2)

Due to the PII collected, the impact level is moderate. The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

16. What involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system? (AR-3)

Intelliworx does not have contractors supporting the Intelliworx system.

In accordance with the contract between FERC and HRworx, LLC (e.g., Intelliworx), the NDA clause in the contract states that "the Contractor [Intelliworx] and all personnel assigned to the contract that require access to the FERC network are required not to divulge to any unauthorized person non-public or confidential information obtained from FERC in performance of their duties under the contract." Intelliworx will be required to sign a Non-Disclosure/Confidentiality Agreement prior to commencement of work.

17. *Is the PII owner advised about what federal agencies or other organizations share or have access to the data? (AR-1)*

Not applicable. Data is not shared through the Intelliworx system nor the FDonline module.

3.6 CONTRACTS, AGREEMENTS, AND OWNERSHIP

18. NIST SP 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this accountability described in contracts with customers? Why or why not? (AR-3)

No. FERC's accountability for the security and privacy of the PII held by Intelliworx has not been described in the contract. However, FERC does not relinquish responsibility for the security and privacy of the data (e.g., PII), but is accountable for the security and privacy of the data collected and stored in the FDonline module.

19. Do contracts with customers establish who has ownership rights over data including PII? (AR-2, AR-3)

Yes. Contracts establish that all clients own their PII data and that Intelliworx owns their intellectual property and proprietary documentation, marked as such.

The contract between FERC and Intelliworx states that "All documentation, electronic data and information collected or generated by the Contractor in support of this contract will be considered Government property and will be returned to the Government at the end of the performance period."

20. Do contracts with customers require that customers notify Intelliworx if the customer intends to populate the service platform with PII? Why or why not? (AR-3)

No. The Intelliworx platform is a software application platform that allows customer agencies to streamline and automate workflows in any number of mission areas. The platform consists of modules. Each module has been analyzed to determine if any elements of that module collect and/or store PII.

21. Do Intelliworx contracts with customers establish record retention responsibilities for both the customer and Intelliworx? (AR-2, AR-3)

Yes. Record retention responsibilities are specified by OGE (FDonline) and are included in contracts with customers.

Record retention responsibilities are provided in question 27 below.

22. Is the degree to which Intelliworx will accept liability for exposure of PII clearly defined in agreements with customers? (AR-3)

In accordance with the contract between FERC and Intelliworx, under the *Cyber Security and Privacy Incident Reporting and Data Breaches* section, Intelliworx will be required to prevent and remedy data breaches, provide FERC with all necessary information and cooperation, and take all other reasonable and necessary steps and precautions to enable FERC to satisfy its data breach reporting duties under applicable law, regulation, or policy in the event, if any, that a breach occurs.

3.7 ACCURACY OF THE PII AND REDRESS

23. Is the PII collected verified for accuracy? Why or why not? (DI-1)

There is automated formatting validation within the software. The information is entered directly from the employee. In addition, the Ethics Division in the FERC General and Administrative Law office verifies stock and retirement funds by researching information provided against the prohibited securities list. Additional verification is conducted online to identify other stock and retirement funds that are prohibited.

In addition, FERC's Human Resources department verifies information provided by the employee.

24. Is the PII current? How is this determined? (DI-1)

The PII is considered to be current as it is entered directly by the individual at the time of onboarding or filing. Individuals are responsible for entering accurate PII and maintaining currency of the data submitted.

25. Is there a process for individuals to have inaccurate PII that is maintained by the system corrected or amended, as appropriate?

Filers within the Intelliworx: FDonline module are required to update their PII on an annual basis when reporting their financial assets. Individual filers can work with the FERC designated ethics administrator to request access to their records and reopen a filing if PII needs to be updated for the current filing year.

3.8 MAINTENANCE AND ADMINISTRATIVE CONTROLS

26. If the system is operated in more than one site, how is consistent use of the PII maintained in all sites? Are the same controls used?

The Intelliworx system operates within and leverages the AWS GovCloud Infrastructure as a Service (IaaS) environment. Intelliworx utilizes the AWS GovCloud IaaS multiple availability zone functionality as the alternate processing site for the Intelliworx system. Both primary and secondary availability zones are within the Intelliworx system FedRAMP authorization boundary where the same controls are implemented and assessed.

27. What are the retention periods of PII for this system? Under what guidelines are the retention periods determined? Who establishes the retention guidelines? (AR-2, AR-3, DM-2)

The data retention requirement for the onboarding module is mandated by Office of Personnel Management (OPM). OPM requires onboarding data to be purged within ninety (90) days, with the exception of user activity/events. The requirements are published in the OPM Entrance on Duty (EOD) Requirements Specifications, section 4.4.3 User Actions Audit Trail and section 4.5.3 Temporary Account Termination: https://www.opm.gov/policy-data-oversight/data-analysis-documentation/enterprise-human-resources-integration/entrance-on-duty/requirements.pdf.

The following general records schedule is adhered to at FERC as it relates to the below records.

GENERAL RECORDS SCHEDULE 2.8: Employee Ethics Records

This schedule covers records documenting the activities of executive branch agency ethics program offices.

Item	Record Description		Disposition Instruction	Disposition Authority
070	Confidential financial disclosure reports. Executive Branch Confidential Financial Disclosure Reports (OGE Form 450) and Confidential Certificates of No New Interests	Reports for individuals not subsequently confirmed by the U.S. Senate.	Temporary. Destroy 1 year after nominee ceases to be under consideration for the position or when no longer needed for active	DAA-GRS2014-00050011

		Legal Citation: 5 CFR 2634.604	investigation, whichever is later. This disposition instruction is mandatory; deviations are not allowed	
071	OGE Form 450 continued	All other reports. Legal Citation: 5 CFR 2634.604	Temporary. Destroy 6 years after receipt of the OGE Form 450 by the agency.	DAA-GRS-2014-00050012

28. What are the procedures for disposition of the PII at the end of the retention period? How long will any reports that contain PII be maintained? How is the information disposed (e.g., shredding, degaussing, overwriting, etc.)? Who establishes the decommissioning procedures? (AR-2, DM-2)

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.

In accordance with the contract between FERC and Intelliworx, when the information is no longer required, this information, data, and/or equipment will be returned to Government control, destroyed, or held until otherwise directed. Destruction of items will be accomplished by following NIST SP 800-88 Revision 1, *Guidelines for Media Sanitization*. The disposition of all data will be at the written direction of the Contracting Officer's Representative (COR). This may include documents returned to Government control, destroyed, or held as specified until otherwise directed. Items returned to the Government will be hand carried or sent by certified mail to the COR.

29. Is the system using new technologies that contain PII in ways that have not previously deployed (e.g., smart cards, caller-ID, biometrics, PIV cards, etc.)?

No.

30. How does the use of this technology affect privacy? Does the use of this technology introduce compromise that did not exist prior to the deployment of this technology?

Not applicable.

31. Is access to the PII being monitored, tracked, or recorded? (AR-4)

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.

32. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision? (TR-2)

The system is not being modified. The applicable system of records notice for this system is OGE/GOVT-2 Executive Branch Confidential Financial Disclosure Reports Privacy Act SORN.

3.9 BUSINESS PROCESSES AND TECHNOLOGY

33. Have the talking points found herein resulted in circumstances that requires changes to business processes?

No.

34. Does the outcome of these talking points require that technology or operational changes be made to the system?

No.

3.10 PRIVACY POLICY

35. Is there a system privacy policy and is it provided to all individuals whose PII you collect, maintain or store? (IP-1, TR-1, TR-3)

Intelliworx has not established a privacy policy for the Intelliworx system.

36. Is the privacy policy publicly viewable? If yes, provide the URL. (TR-1, TR-3)

Intelliworx has not established a privacy policy for the Intelliworx system.

3.11 SIGNATURES

The information found herein has been documented by *SecureIT* and has been reviewed by the Intelliworx, Chief Privacy Officer for accuracy.

CHRISTINA HANDLEY Digitally signed by CHRISTINA HANDLEY
Date: 2019.12.04 11:04:08 -05'00'

FERC Senior Agency Official for Privacy Signature

Name **Christina Handley** **Date** **11/22/2019**

Assessor Signature

Name **Corey Clements** **Date** **11/22/2019**

Laurence Kirby 12/16/2019

Chief Privacy Officer Signature

Name **Laurence Kirby** **Date** **11/22/2019**

4 ACRONYMS

The master list of FedRAMP acronym and glossary definitions for all FedRAMP templates is available on the FedRAMP website Documents page under Program Overview Documents.

Please send suggestions about corrections, additions, or deletions to info@fedramp.gov.