Date of Approval: **February 06, 2023**

PIA ID Number: **7210**

SYSTEM DESCRIPTION

Enter the full name and acronym for the system, project, application and/or database.

Enterprise Secure Large File Transfer - Kiteworks, Kiteworks (ESLFT)

Is this a new system?

Yes

What governance board or Executive Steering Committee (ESC) does this system report to? Full name and acronym.

ES Governance Board

Current ELC (Enterprise Life Cycle) Milestones:

Project Initiation/Milestone 1

Domain Architecture/Milestone 2

Preliminary Design/Milestone 3

Detailed Design/Milestone 4A

System Development/Milestone 4B

System Deployment/Milestone 5

Is this a Federal Information Security Management Act (FISMA) reportable system?

No

GENERAL BUSINESS PURPOSE

What is the general business purpose of this system? Provide a clear, concise description of the system, application or database, the reason for the system, and the benefits to the IRS to use the information, and how the information will be used.

Kiteworks, a managed service provider with cloud-based SaaS solution, has been selected an Enterprise Solution for secure large file transfer. Kiteworks will eliminate the need to bring in other tools to meet the existing gaps in the IRS Enterprise large file transfer space; and reduce resource demand constraints that the IRS faces today to execute its many file sharing objectives.

PII DETAILS

Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information: or any other type of Sensitive but Unclassified (SBU) information or PII such as information about IRS employees or outside stakeholders?

Yes

Does the system use, collect, receive, display, store, maintain, or disseminate Social Security Numbers (SSN's) or tax identification numbers (i.e., last 4 digits, etc.)?

Yes

What types of tax identification numbers (TIN) apply to this system?

Social Security Number (SSN)

List the approved Treasury uses of the SSN:

Legal/statutory basis (e.g., where collection is expressly required by statute)

Law enforcement and intelligence purposes

Explain why the authorized use(s) above support the new or continued use of SSNs (or tax identification numbers).

There is a legal/statutory basis (tax information (file) is transmitted with the Department of Justice (DOJ) for tax related cases.

Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of SSN's (or tax identification numbers).

None. Tax return information may be shared with state/federal agencies responsible for tax information. In this case, tax information (file) is transmitted via file transfer to the Department of Justice (DoJ).

Employer Identification Number

Other Taxpayer Identification Number

Does this system use, collect, receive, display, store, maintain or disseminate other (non-SSN) PII (i.e., names, addresses, etc.)?

Yes

Specify the PII Elements:

Name
Mailing address
Phone Numbers
E-mail Address
Date of Birth
Place of Birth
Standard Employee Identifier (SEID)
Mother's Maiden Name
Protection Personal Identification Numbers (IP PIN)
Internet Protocol Address (IP Address)
Criminal History
Medical Information
Certificate or License Numbers
Vehicle Identifiers
Passport Number
Alien Number
Financial Account Numbers
Photographic Identifiers
Biometric Identifiers
Employment Information
Tax Account Information
Centralized Authorization File (CAF)

Does this system use, collect, receive, display, store, maintain, or disseminate SBU information that is not PII?

Yes

Specify the types of SBU from the SBU Types List:

Official Use Only (OUO) or Limited Official Use (LOU) Information designated as OUO, or LOU is information that: is exempt under one of the statutory Freedom of Information Act exemptions; is prohibited by other laws or regulations; would significantly impede the agency in carrying out a responsibility or function; or would constitute an unwarranted invasion of privacy.

Protected Information Information which if modified, destroyed, or disclosed in an unauthorized manner could cause loss of life, loss of property or funds by unlawful means, violation of personal privacy or civil rights, gaining of an unfair procurement advantage by contractors bidding on government contracts, or disclosure of proprietary information entrusted to the Government.

Criminal Investigation Information Information concerning IRS criminal investigations or the agents conducting the investigations.

Are there other types of SBU/PII used in the system?

Yes

Describe the other types of SBU/PII that are applicable to this system.

Yes - Taxpayer Records, Non SBU information could be transmitted such as shipping information.

Cite the authority for collecting SBU/PII (including SSN if relevant).

PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, & 6012e(a)

SSN for tax returns and return information is Internal Revenue Code Section 6109

Has the authority been verified with the system owner?

Yes

BUSINESS NEEDS AND ACCURACY

Explain the detailed business needs and uses for the SBU/ PII, and how the SBU / PII is limited only to that which is relevant and necessary to meet the mission requirements of the system. If SSNs (or tax identification numbers) are used, explicitly explain why use of SSNs meets this criteria. Be specific.

In Release 1 the IRS users will leverage FedRAMP certified Kiteworks native capabilities to support IRS Chief Counsel's (CC) and Whistleblowers Office (WO) need to have a secure large file transfer solution in place for January 31, 2023, Release 1 to support CC's ongoing handling of the civilian cases with DOJ when the current solution expires and to support WO's office to virtually submit the paperwork by the Whistleblowers. The files transferred between / among the IRS and external entities would likely contain data supporting critical tax administration and compliance functions and that would include Social Security Numbers (SSN's) or tax identification numbers. Kiteworks Managed Services end-users such as Chief Counsel and the Whistleblower Office (WBO) will utilize the Custom off the Shelf (COTS) product managed service offering in the routine course of business to provide data, casefile info, etc., all of which would likely include PII, and their business practices would include collaboration with entities that require the SSN. In the delivery of tax administration services, governmental benefits, law enforcement activities, and judicial or intelligence gathering pursuits, the IRS's compliance lines of business which include the Whistleblowers Office and Chief Counsel (with whom the Department of Justice interacts heavily) -- all have a legal / judicial / statutory basis to collect/share SSNs.

How is the SBU/PII verified for accuracy, timeliness, and completion?

SBU/PII is verified for authentication and authorization access, access controls, and log files. Every file transfer is verified via sender and receiver in an isolated, secure private cloud. Each file has a time stamp. The administrator has the ability configure the system to delete the files immediately upon receipt.

PRIVACY ACT AND SYSTEM OF RECORDS

The Privacy Act requires Federal agencies that maintain a system of records to publish systems of records notices (SORNs) in the Federal Register for records from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence. The Privacy Act also provides for criminal penalties for intentional noncompliance.

Does your application or this PCLIA system pertain to a group of any record from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence? An identifier may be a symbol, voiceprint, SEID, or other personal identifier that is used to retrieve information.

No

RESPONSIBLE PARTIES

Identify the individuals for the following system roles:

Official Use Only

INCOMING PII INTERFACES

Does the system receive SBU/PII from other systems or agencies?

Yes

Does the system receive SBU/PII from IRS files and databases?

No

Does the system receive SBU/PII from other federal agency or agencies?

Yes

For each federal interface, identify the organization that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Name: Department of Justice
Transmission Method: Secure External File Transfer
ISA/MOU: Yes

Does the system receive SBU/PII from State or local agency (-ies)?

No

Does the system receive SBU/PII from other sources?

No

Does the system receive SBU/PII from Taxpayer forms?

No

Does the system receive SBU/PII from Employee forms (e.g., the I-9)?

No

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

Yes

Does this system disseminate SBU/PII to other IRS Systems?

Yes

Identify the full name and acronym of the IRS system(s) that receive SBU/PII from this system.

System Name: Criminal Investigation (CI)
Current PCLIA: No
SA&A: No

System Name: Small Business/Self Employed (SBSE)
Current PCLIA: No
SA&A: No

System Name: Tax Exempt Government Entities (TEGE)
Current PCLIA: No
SA&A: No

System Name: Chief Counsel (CC)
Current PCLIA: No
SA&A: No

System Name: Large Business and International (LB&I)
Current PCLIA: No
SA&A: No

Identify the authority.

Internal work for case related purposes.

For what purpose?

To support critical tax administration and compliance functions.

Does this system disseminate SBU/PII to other Federal agencies?

Yes

Identify the full names of the federal agency(s) that receive SBU/PII from this system, and if there is an Inter-Agency Agreement (ISA) / Memorandum of Understanding (MOU).

Organization Name: Department of Justice (DOJ)
Transmission Method: Secure External File Transfer
ISA/MOU: Yes

Organization Name: Alcohol and Tobacco Tax and Trade Bureau (TTB)
Transmission Method: Secure External File Transfer
ISA/MOU: Yes

Identify the authority.

Exchange agreement, IRC 6103(h)(4) and 6103(k)(13)

Identify the Routine Use in the applicable SORN (or Privacy Act exception).

N/A

For what purpose?

To support critical tax administration and compliance functions.

Does this system disseminate SBU/PII to State and local agencies?

No

Does this system disseminate SBU/PII to IRS or Treasury contractors?

No

Does this system disseminate SBU/PII to other Sources?

No

PRIVACY SENSITIVE TECHNOLOGY

Does this system use social media channels?

No

Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.?

Yes

Briefly explain how the system uses the referenced technology.

Kiteworks provides a GPS function via IP Address tracking to confirm location of the file sent/received and sender/receiver of the file. Visualization and dashboarding are done so that it can determine possible data exfiltration when an unusual file is downloaded to an unusual location.

Does the system use cloud computing?

Yes

Is the cloud service provider (CSP) Federal Risk and Authorization Management Program (FedRAMP) certified?

Yes

Date Certified.

6/1/2017

Please identify the ownership of the CSP data.

IRS

Does the CSP allow auditing?

Yes

Who audits the CSP Data?

IRS

What is the background check level required for CSP?

Moderate

Is there a breach/incident plan on file?

No

When will Breach/Incident plan be available?

12/22/2022

Privacy laws (including access and ownership) can differ in other countries. This cloud will be Continental US (CONUS) only for:

Storage
Transmission
Maintenance

Does this system/application interact with the public?

Yes

Was an electronic risk assessment (e-RA) conducted on the system/application?

Not Applicable

Please explain.

Managed service

INDIVIDUAL NOTICE AND CONSENT

Was/is notice provided to the individual prior to collection of information?

No

Why not? If information is not collected directly from an individual, please discuss the factors considered in deciding to collect information from third party sources.

Information is not collected directly from an individual. The files uploaded to the staging server are for tax administration purposes and notice, consent and due process are provided in the tax forms instructions, and pursuant to 5 USC.

Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information?

No

Why not?

Information is not collected directly from an individual.

How does the system or business process ensure 'due process' regarding information access, correction, and redress?

Information is not collected directly from an individual.

INFORMATION PROTECTION

Identify the owner and operator of the system (could be IRS owned and operated; IRS owned, contractor operated; contractor owned and operated).

IRS Owned and Operated

The following people have access to the system with the specified rights:

IRS Employees

Users: Read Write

Managers: Read Write

System Administrators: Administrator

IRS Contractor Employees

Contractor Users: Read Write

Contractor Managers: Read Only

How is access to SBU/PII determined and by whom?

Access to the data to be transferred will be determined via the BEARS System. Access is granted only to the individual folder they need to view and time limits are set. The files will expire if not accessed within the allotted timeframe.

RECORDS RETENTION SCHEDULE

Are these records covered under a General Records Schedule (GRS, IRS Document 12829), or has the National Archives and Records Administration (NARA) approved a Records Control Schedule (RCS, IRS Document 12990) for the retention and destruction of official agency records stored in this system?

Yes

How long are the records required to be held under the corresponding GRS or RCS, and how are they disposed of? In your response, please provide the GRS or RCS chapter number, the specific item number, and records series title.

Kiteworks Secure External File Transfer Service is non-recordkeeping for IRS purposes. It is a platform for secure communications and information sharing between the IRS and Federal Agencies or external Trading Partners. It is not the official IRS repository for any data or documents. The IRS can control the retention or destruction of original data. The IRS can erase the summoned records from our staging server within 24 hours after the records are ready to be retrieved. There is no change to the IRS retention of records.

SA&A OR ASCA

Has the system been through SA&A (Security Assessment and Authorization) or ASCA (Annual Security Control Assessment)?

In-process

When is the anticipated date of the SA&A or ACS completion?

2/28/2023

Describe the system's audit trail.

Content communication services enables IRS cybersecurity to comprehensively monitor third-party traffic for breaches and compliance violations, starting with a complete, centralized log of all files, user, and administrator activity. IRS will use the log data to create clear and complete real-time visualizations that answer the most important security questions about the information entering and leaving the organization to provide forensic reporting to aid investigators.

PRIVACY TESTING

Does the system require a System Test Plan?

Yes

Is the test plan completed?

No

When is the test plan scheduled for completion?

12/22/2023

Describe what testing and validation activities have been conducted or are in progress to verify and validate that the applicable Privacy Requirements (listed in header) have been met?

The Kiteworks managed service platform will leverage a FedRAMP private cloud for compliance with IRS standards and NIST 800-53 controls to form the security foundation to IRS specifications. These include requirements from Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Standards (PCI), and System and Organization Controls (SOC 2), to Family Educational Rights & Privacy (FERPA), International Traffic and Arms Regulations (ITAR), and NIST 800-171 common controls. FedRAMP includes these controls for periodic compliance audits, continuous monitoring and yearly third-party audits and incorporates FIPS 140-2 compliant cryptology.

SBU DATA USE

Does this system use, or plan to use SBU Data in Testing?

No

NUMBER AND CATEGORY OF PII RECORDS

Identify the number of individual records in the system for each category:

IRS Employees: Under 50,000

Contractors: Under 5,000

Members of the Public: Under 100,000

Other: No

CIVIL LIBERTIES

Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment?

No

Is the system information used to conduct 'data-mining' as defined in the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 804?

No

Will this system have the capability to identify, locate, and monitor individuals or groups of people?

No

Does computer matching occur?

No

ACCOUNTING OF DISCLOSURES

Does the system include or require disclosure of tax or employee information to anyone other than IRS employees in the performance of their duties, or to the person to whom the information pertains or to a 3rd party pursuant to a Power of Attorney, tax, or Privacy Act consent?

Yes

Does the system have a process in place to account for such disclosures in compliance with IRC §6103(p) (3) (A) or Subsection (c) of the Privacy Act? Contact Disclosure to determine if an accounting is required.

Yes