Date of Approval: 12/20/2017 PIA ID Number: **2946**

A. SYSTEM DESCRIPTION

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

2. Is this a new system? Yes

3. Check the current ELC (Enterprise Life Cycle) Milestones (select all that apply)

No	Vision & Strategy/Milestone 0
No	Project Initiation/Milestone 1
No	Domain Architecture/Milestone 2
No	Preliminary Design/Milestone 3
No	Detailed Design/Milestone 4A
No	System Development/Milestone 4B
No	System Deployment/Milestone 5
Yes	Operations & Maintenance (i.e., system is currently operational)

4. Is this a Federal Information Security Management Act (FISMA) reportable system? No

A.1 General Business Purpose

5. 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. The purpose of the SharePoint software is to provide a backbone for team collaboration sites is to store, maintain, and share information as it correlates to the objectives and goals of the Internal Revenue Service (IRS) Business Units. It provides the tools to maintain and manage the IRS SharePoint platform, technical documentation, plans, policies, standard operating procedures, and allows users to leverage built-in tools for manipulating data and presentations. It will also house day-to-day materials to assist the teams with tracking progress including meeting minutes, agenda and internal knowledge documentation that assist in storing key internal knowledge for customers looking to create a SharePoint collection. SharePoint will host functionality such as Access service, Versioning of documents, and eventually (currently planned) My Sites. This includes the following default functionality: Profiles, Newsfeed, and Content storing/sharing. Information owners are responsible for the data they share through the system and will complete a separate SharePoint Privacy Impact Assessment (SP PIA) as needed for any site collections storing Sensitive But Unclassified (SBU) or Personally Identifiable Information (PII) data.

B. PII DETAIL

6. Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any type of Sensitive but Unclassified (SBU) or Personally Identifiable Information (PII)? Yes

6a. If **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.)? No

If **yes**, check who the SSN (or tax identification number) is collected on.

No	On Primary	No	On Spouse	No	On Dependent

6b. Does this system contain other (non-SSN) PII that it uses, collects, receives, displays, stores, maintains, or disseminates? (i.e. Names, addresses, etc.) Yes

If **yes**, specify the information.

Selected	PII Element	On Primary	On Spouse	On Dependent
Yes	Name	No	No	No
Yes	Mailing address	No	No	No
Yes	Phone Numbers	No	No	No
Yes	E-mail Address	No	No	No
No	Date of Birth	No	No	No
No	Place of Birth	No	No	No
Yes	SEID	No	No	No
No	Mother's Maiden Name	No	No	No
No	Protection Personal Identification Numbers (IP PIN)	No	No	No
Yes	Internet Protocol Address (IP Address)	No	No	No
No	Criminal History	No	No	No
No	Medical Information	No	No	No
No	Certificate or License Numbers	No	No	No
No	Vehicle Identifiers	No	No	No
No	Passport Number	No	No	No
No	Alien (A-) Number	No	No	No
No	Financial Account Numbers	No	No	No
No	Photographic Identifiers	No	No	No
No	Biometric Identifiers	No	No	No
No	Employment (HR) Information	No	No	No
No	Tax Account Information	No	No	No

6c. Does this system contain SBU information that is not PII, it uses, collects, receives, displays, stores, maintains, or disseminates? Yes

If **yes**, select the types of SBU

Selected	SBU Name	SBU Description
No	Agency Sensitive Information	Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission
Yes	Procurement sensitive data	Contract proposals, bids, etc.
No	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.
Yes	Proprietary data	Business information that does not belong to the IRS
No	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
Yes	Physical Security Information	Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities
No	Criminal Investigation Information	Information concerning IRS criminal investigations or the agents conducting the investigations.

.

6d. Are there other types of SBU/PII used in the system? No

If **yes**, describe the other types of SBU/PII that are applicable to this system.

6e. Cite the authority for collecting SBU/PII (including SSN if relevant)

No	PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(a)
No	SSN for tax returns and return information is Internal Revenue Code Section 6109
No	SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397
Yes	PII for personnel administration is 5 USC
No	PII about individuals for Bank Secrecy Act compliance 31 USC
No	Information by CI for certain money laundering cases may be 18 USC

6f. Has the authority been verified with the system owner? Yes

B.1 BUSINESS NEEDS AND ACCURACY

7. 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 the criteria. Be specific. Standard Employee Identifier (SEID), Name, E-mail are used to grant access to the site collections. Phone number and E-mails are used for communication purposes. IP Addresses to track the different site collections the SharePoint Program Management Office manages. Procurement and security information is only used for high-level executive communication and tracking; it is restricted to only those users.

8. How is the SBU/PII verified for accuracy, timeliness, and completeness? Explain how steps are taken to ensure that all information maintained by the system that is used by IRS to make any adverse determination about an individual's rights, benefits, and/or privileges is maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination. SharePoint user information is obtained via a daily automatic synchronization with the IRS Active Directory (AD). Any corrections to the data should be handled per standard processes for updating the IRS AD.

C. PRIVACY ACT AND SYSTEM OF RECORDS

9. Are 10 or more records containing SBU/PII maintained, stored, and/or transmitted by or through this system? Yes

9a. If **yes**, are records in the system retrieved by any personal identifier (e.g., name, SSN, Photograph, IP Address) for an individual? Yes

If **yes**, is there a System of Records Notice(s) or SORNs that addresses the PII records in this system? Yes

If **yes**, enter the SORN number(s) and the complete the name of the SORN.

SORNS Number	SORNS Name
Treas/IRS 36.003	General Personnel and Payroll Records
Treas/IRS 00.001	Correspondence
Treas/IRS 34.037	Audit Trail and Security Records System

If **yes**, does the System of Records Notice(s) (SORN) published in the Federal Register adequately describe the records as required by the Privacy Act? Yes

D. RESPONSIBLE PARTIES

10. Identify the individuals for the following system roles. ## Official Use Only

E. INCOMING PII INTERFACES

11. Does the system receive SBU/PII from other system or agencies? No

F. PII SENT TO EXTERNAL ORGANIZATIONS

12. Does this system disseminate SBU/PII? No

G. PRIVACY SENSITIVE TECHNOLOGY

13. Does this system use social media channels? No

14. Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.? No

15. Does the system use cloud computing? No

16. Does this system/application interact with the public? No

H. INDIVIDUAL NOTICE AND CONSENT

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

17a. If **yes**, how is notice provided? Was the individual notified about the authority to collect the information, whether such is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects, if any, if they decide not to provide any of the requested information? Access to SharePoint and the creation of SharePoint user records is automatic based on the user's completion of the an Online-5081 request for access to the IRS network and agreement to those terms and conditions. This is a purely internal system. It does not make any determinations on its own. Any individual information is received from a system that provides employees with notice and rights to consent and/or amend, as needed. Notice comes through such communications as the Privacy Act notification on Human Resource Connect (HR Connect) and e-Performance, Single Entry Time Reports (SETR), and other personnel systems. Employee rights are covered through appropriate legal and National Treasury Employees Union (NTEU) contractually negotiated process for remediation.

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

18a. If **yes**, describe the mechanism by which individuals indicate their consent choice(s): Employee rights are covered through appropriate legal and National Treasury Employees Union (NTEU) contractually negotiated process for remediation.

19. How does the system or business process ensure due process regarding information access, correction and redress? All corrections or errors should be handled through the IRS standard process to correct errors with the IRS Active Directory.

I. INFORMATION PROTECTION

20. 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

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

IRS Employees? Yes

IRS Employees?	Yes/No	Access Level (Read Only/Read Write/ Administrator)
Users	Yes	Read and Write
Managers	Yes	Read and Write
Sys. Administrators	Yes	Administrator
Developers	Yes	Administrator

Contractor Employees? Yes

Contractor Employees?	Yes/No	Access Level	Background Invest. Level
Contractor Users	Yes	Read and Write	Moderate
Contractor Managers	Yes	Read and Write	Moderate
Contractor Sys. Admin.	Yes	Administrator	Moderate
Contractor Developers	Yes	Administrator	Moderate

21a. How is access to SBU/PII determined and by whom? Site Collection Administrators and Site Owners are responsible for the data they share through the system and will complete a separate SharePoint Privacy Impact Assessment (SP PIA), as needed, for any SharePoint Site Collection storing SBU or PII data.

21b. If computer matching occurs, can the business owner certify that it meets requirements of IRM 11.3.39 Disclosure of Official Information, Computer Matching & Privacy Protection Act?

Not Applicable

I.1 RECORDS RETENTION SCHEDULE

22. Are these records covered under the General Records Schedule (GRS), or have a National Archives and Records Administration (NARA) archivist approved a Record Control Schedule (RCS) for the retention and destruction of official agency records stored in this system? Yes

22a. If **yes**, how long are the records required to be held under the corresponding RCS and how are they disposed of? In your response, please include the complete IRM number 1.15.XX and specific item number and title. Appropriate Records Control Schedules will be applied to records at Site Collection levels and not at the SharePoint farm level because the platform will include records series from Business Units across the service. User logs and access logs are maintained according to General Records Schedule (GRS) 3.1: General Technology Management Records, Item 020 for Information technology operations and maintenance records. System Documentation logs are maintained under GRS 3.1, Item 051.

I.2 SA&A OR ECM-R

23. Has the system been through SA&A (Security Assessment and Authorization) or ECM-R (Enterprise Continuous Monitoring Reauthorization)? No

23c. If **no**, is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements? Yes

23.1 Describe in detail the system s audit trail. SharePoint versioning functionality has been enabled to track history of information uploaded and updated. Additional options to audit access to information are available both within the SharePoint Administrative capabilities and an add-on tool Quest Site Administrator Reports. These enable auditing of the access, or ability to access (via permissions), sites collections which are the containers of potential PII/SBU.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? No

24c. If **no**, please explain why. SharePoint is a platform. System Test Plans are prepared by Site Collection Managers/Owners that seek to alter their SharePoint capabilities from the base configuration, The SharePoint Program Management Office has authored related technical documentation, plans, policies, standard operating procedures, governance materials and executive level/BU presentation.

K. SBU Data Use

25. Does this system use, or plan to use SBU Data in Testing? No

L. NUMBER AND CATEGORY OF PII RECORDS

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

26a. IRS Employees: More than 100,000
26b. Contractors: More than 10,000
26c. Members of the Public: Not Applicable
26d. Other: Yes

If **other**, identify the category of records and the number of corresponding records (to the nearest 10,000). Access may be granted to TIGTA or GAO for audit access.

M. CIVIL LIBERTIES

27. Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment? No

28. Is the system information used to conduct data-mining as defined in the *Implementing the 9/11 Commission Recommendations Act of 2007, Public Law 110-53, Section 804?* No

29. Will this system have the capability to identify, locate, and monitor individuals or groups of people? No

N. ACCOUNTING OF DISCLOSURES

30. 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? No

End of Report