Date of Approval: August 23, 2017 PIA ID Number: **2763**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Stakeholder Partnerships, Education & Communication Total Relationship Management, SPECTRM

2. Is this a new system? No

2a. If **no**, is there a PIA for this system? Yes

If **yes**, enter the full name, acronym, PIA ID Number and milestone of the most recent PIA.

Stakeholder Partnerships, Education & Communication Total Relationship Management, SPECTRM, ID 933

Next, enter the **date** of the most recent PIA. 8/14/2014

Indicate which of the following changes occurred to require this update (check all that apply).

No	Addition of PII
No	Conversions
No	Anonymous to Non-Anonymous
No	Significant System Management Changes
No	Significant Merging with Another System
No	New Access by IRS employees or Members of the Public
No	Addition of Commercial Data / Sources
No	New Interagency Use
No	Internal Flow or Collection

Were there other system changes not listed above? No

If yes, explain what changes were made.

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

Yes	Vision & Strategy/Milestone 0
Yes	Project Initiation/Milestone 1
Yes	Domain Architecture/Milestone 2
Yes	Preliminary Design/Milestone 3
Yes	Detailed Design/Milestone 4A
Yes	System Development/Milestone 4B
Yes	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.

Stakeholder, Partnerships, Education & Communication (SPEC) Total Relationship Management (SPECTRM) is a comprehensive system that gives SPEC and its employees the ability to manage relationships with its partnering organizations, volunteers, and external stakeholders in support of the Volunteer Income Tax Assistance (VITA) and Tax Counseling for the Elderly (TCE) programs. The system is a web-based application that is deployed nationwide to SPEC personnel. Access is limited to IRS SPEC users via office Local Area Network (LAN) in approximately 95 IRS offices or via Enterprise Remote Access Project (ERAP) from remote locations.

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

If **yes**, check all types SSN s (or tax identification numbers) that apply to this system:

No	Social Security Number (SSN)
No	Employer Identification Number (EIN)
No	Individual Taxpayer Identification Number (ITIN)
No	Taxpayer Identification Number for Pending U.S. Adoptions (ATIN)
No	Practitioner Tax Identification Number (PTIN)

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

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	Yes	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
No	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
No	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.
No	Proprietary data	Business information that does not belong to the IRS
Yes	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
No	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

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 this criteria. Be specific.

VITA/TCE volunteer tax preparation partners and the corresponding sites operate using volunteers who must certify their tax compliance knowledge to be eligible to prepare returns at the VITA/TCE sites. Partnering non-profit organizations participating in the VITA/TCE program must submit information containing PII data related to primary points of contact for the partner and any sites operated. VITA/TCE sites must be individually identified, so a Site Identification Number (SIDN) generated either by the partner (according to agree upon guidelines) or by Spec's Management Information System (MIS) known as SPECTRM, is stored/included in many SPEC documents and forms. All these data items are required to manage the VITA/TCE programs, allowing for resource management and operational accountability. Data from the following forms is stored in the data fields of the SPECTRM MIS: Form 13715 SPEC Volunteer Site Information Sheet; Form 14099 SPEC Financial Education and Asset Building Partner Assessment Tool; Form 13206 SPEC Volunteer Assistance Report; Form 13615 Volunteer Standards of Conduct Agreement; Form 13632 Property Loan Agreement; Form 13533 VITA/TCE Partner Sponsor Agreement. These data items are collected under 5 United States Code (USC) 301 and 26 USC 7801. These data items are received from the relevant partners and volunteers, and are inputted and updated by Wage & Investment (WI) Customer Assistance, Relationships and Education (CARE) SPEC employees assigned as the Relationship Manager (RM) for the specific partners.

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

The data containing PII/SBU information is largely inputted and maintained at the SPEC territory level. There are various Internal Revenue Manual (IRM) specified deadlines each year that RMs are required to update and/or renew the information. Verification occurs each year in the Fall in preparation for the filing season. RMs will solicit the coming year's information for accuracy and updates through submission of forms for the coming season cycle, containing the most current data from the partner. This information is inputted into SPECTRM then submitted to the Territory Manager for approval and signature. SPECTRM uses a Post of Duty and role-based security model that allows read/write access to only those individuals who need it for the territories and areas in the system. This is internal, operational data for SPEC and is not disseminated outside of SPEC with the following exceptions: 1) VITA/TCE site information cleansed of all PII/SBU data is posted

to the Free Tax Prep locator tool through an extract file, accessible from IRS.gov. 2) Valid SIDNs and site names are shared through an extract file transported nightly to the e-Services Third-Party Data Store system using the Electronic File Transfer Utility (EFTU). No PII/SBU data is included. 3) Valid SIDNs and site names are shared through an extract file transported weekly to the RPVUE command code using the EFTU. No PII/SBU data is included.

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 10.004	Stakeholder Relationship Management an
Treas./IRS 36.003	General Personnel and Payroll Records

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? Yes

11a. If **yes**, does the system receive SBU/PII from IRS files and databases? No

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

11c. Does the system receive SBU/PII from State or local agency (-ies)? No

11d. Does the system receive SBU/PII from other sources? No

11e. Does the system receive SBU/PII from **Taxpayer** forms? Yes

If **yes**, identify the forms

Form Number	Form Name
13615	Volunteer Standards of Conduct Agreement
13206	Volunteer Assistance Summary Report
13715	Volunteer Site Information Sheet
13533	VITA/TCE Partner Sponsor Agreement
13632	Property Loan Agreement
14099	SPEC Partner/Site Financial Education & Asset Building Assessment

11f. Does the system receive SBU/PII from **Employee** forms (such as the I-9)? 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?
Volunteer PII is submitted to SPEC RMs at the territory level through Form 13615. The Form 13615 data collects the basic PII of the volunteer, and allows them to certify their training requirements as a volunteer. Form 13615 includes sites of the Privacy Act and 5 USC 301 authority for the collection of the information. The information is voluntary, as this is a volunteer program, therefore individuals who do not want to provide the information can choose not to volunteer for the VITA/TCE program. The use of the information is also specified in Form 13615.

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):
The VITA/TCE program is strictly a volunteer system, so any individuals who do not want to share the basic PII as part of the Form 13615 submission can choose not to participate. Submission of the Form 13615 includes the volunteer's consent to the use of the PII as specified in the VITA/TCE program.

19. How does the system or business process ensure due process regarding information access, correction and redress?
Partnering organizations sponsoring the volunteers submit the Form 13615 for the volunteers operating at their free tax preparation locations under the VITA/TCE program. WI-CARE SPEC RM at the territory level review the Form 13615 information, and work with the partner/volunteer to address any errors found by the RM or raised by the partner/volunteer. Issues can be raised to the Territory Manager as appropriate, but this is rarely necessary.

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	No	

Contractor Employees? No

21a. How is access to SBU/PII determined and by whom? Access to the SPECTRM is managed using multiple layers. An approved Online 5081 (OL5081) request places authorized users in the Active Directory domain group controlling general access to SPECTRM. The user account created in SPECTRM uses a role-based security model to assign users access to data specific to their responsibilities. Inherited LAN authentication identifies the user and limits their access to data based upon the geographic scope of their SPEC Territory for field employees, Area for Area Analysts (READ ONLY), or Headquarters (HQ) for SPEC HQ staff (READ ONLY). Change/Read/Update/Delete permissions for any records in SPECTRM are enforced based on the user's role in each module. The Contact module houses the PII data in SPECTRM, inputted from Form 13615 information submitted to the local RM in SPEC.

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? No

22b. If **no**, how long are you proposing to retain the records? Please note, if you answered no, you must contact the IRS Records and Information Management Program to initiate records retention scheduling before you dispose of any records in this system.

SPECTRM is unscheduled. W&I and the IRS Records Office will work together to draft a request for records disposition authority for SPECTRM and associated records. When approved by the National Archives and Records Administration, disposition instructions for SPECTRM inputs, system data, outputs, and system documentation will be published in Records Control Schedule (RCS) Document 12990 under RCS 29 for Tax Administration – Wage and Investment, exact item number to be determined.

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)? Yes

23a. If **yes**, what date was it completed? 1/27/2010

23.1 Describe in detail the system s audit trail. SPECTRM was developed in-house by Information Technology-Application Development (IT-AD). During the development Enterprise Life Cycle (ELC) process, SPECTRM was evaluated under a Security Assessment & Authorization (Certification & Accreditation (C&A) at the time) and received an Authority to Operate memo from Cybersecurity on 1/27/2010. As of 6/1/2010, the Security Program Management Office reclassified the SPECTRM application as a non-Federal Information Security Management Act reportable system (FISMA). All SA&A certified controls were left in place, although the application does not follow the full continuous monitoring protocols as a non-FISMA reportable system. SPEC Headquarters annually recertifies user access to SPECTRM through the OL5081 system. SPECTRM application virtual Wintel servers fall under the General Support Services-30 overall security environment, and are subject to standard security and trace monitoring applied to all Wintel application and web servers on the IRS domain.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? Yes

24b. If **yes**, Is the test plan in process or completed: Completed

24.3 If **completed/ or in process,** 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? SPECTRM access is on a need to know/assigned duties basis, using the OL5081 system and domain groups, and SPECTRM's POD/Role-based security to limit access to PII/SBU. During the original C&A of SPECTRM, a ELC System Test Plan was executed. Test user accounts were created using a combination of PODs and roles for each of the seven modules (Contact, Partners, Sites, Site Quality, Equipment, Production, and Software Orders) in the system. SPECTRM project team members then tested each role within each module to determine the

systems enforcement of record access based on the designed limitations. These included: Read-Only, Record Level, Territory Level, Territory Manager, Area Analyst, HQs, and Application Administration roles. Test plan scenarios were used to determine if roles were able to bypass the designed limitations so as to ensure access to PII/SBU fell within the authorized boundaries. Any issues found were corrected and the SPECTRM system was determined to be operating according to the system test plan expected results.

24b.1. If **completed**, where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)? The System Test Plan for SPECTRM is part of the ELC documentation, and is stored with the rest of the ELC artifacts on the Doc-IT system. The folders are managed by the IT-AD Customer Service branch.

24b.2. If **completed**, were all the Privacy Requirements successfully tested? Yes

24.2 If **completed**, are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved? No

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:	Under 50,000
26b. Contractors:	Not Applicable
26c. Members of the Public:	Under 100,000
26d. Other:	No

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