

Date of Approval: **February 21, 2023**

PIA ID Number: **7525**

## **SYSTEM DESCRIPTION**

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

Stakeholder Partnerships, Education and Communication, SPECTRM

*Is this a new system?*

No

*Is there a PCLIA for this system?*

Yes

*What is the full name, acronym, and milestone of the most recent PCLIA?*

IRS Stakeholders, Partnerships, Education and Comm, SPECTRM, O&M, 4740

*What is the approval date of the most recent PCLIA?*

2/27/2020

*Changes that occurred to require this update:*

Expiring PCLIA

*Were there other system changes not listed above?*

Yes

*What were those changes?*

Changes were made to address 508 compliance, Microsoft Edge compatibility and implementation of SSL/HTTPS: for SPECTRM's web-based user interface.

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

Customer Service Division (CSD) Board

*Current ELC (Enterprise Life Cycle) Milestones:*

Operations & Maintenance (i.e., system is currently operational)

*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.*

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 90 IRS offices or via Enterprise Remote Access Project (ERAP) from remote locations.

## **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.)?*

No

*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  
Standard Employee Identifier (SEID)

*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:*

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.

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

No

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

PII for personnel administration is 5 USC

*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.*

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 agreed 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.

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

The data containing PII/SBU information is largely input 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 (POD) 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 Information Data Retrieval System (IDRS) RVPUE (not an acronym) command code using the Enterprise File Transfer Utility (EFTU). No PII/SBU data is included.

## **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.*

Yes

*Identify the Privacy Act SORN(s) that cover these records.*

IRS 10.004 Stakeholder Relationship Management and Subject Files

IRS 36.003 General Personnel and Payroll Records

## **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?*

No

*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?*

Yes

*Please identify the form number and name:*

Form Number: 13615

Form Name: Volunteer Standards of Conduct Agreement

Form Number: 13206

Form Name: Volunteer Assistance Summary Report

Form Number: 13715

Form Name: Volunteer Site Information Sheet

Form Number: 13533

Form Name: VITA/TCE Partner Sponsor Agreement

Form Number: 13632

Form Name: Property Loan Agreement

Form Number: 14099

Form Name: SPEC Partner/Site Financial Education & Asset Building Assessment

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

No

## **DISSEMINATION OF PII**

*Does this system disseminate SBU/PII?*

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.?*

No

*Does the system use cloud computing?*

No

*Does this system/application interact with the public?*

No

## **INDIVIDUAL NOTICE AND CONSENT**

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

Yes

*How is notice provided? Was the individual notified about the authority to collect the information, whether disclosure is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects on the individual, if any, if they decide not to provide all or 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.

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

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.

*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.

## **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 Only  
Contractor Developers: Read Write

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

Access to the SPECTRM is managed using multiple layers. An approved BEARS 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.

## **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.*

RCS 29 Item 440-SPEC (Stakeholder Partnerships, Education and Communication) Grant Application Files and Cooperative Agreements. (a) SPEC-rejected applications. AUTHORIZED DISPOSITION Cut off at end of calendar year (in which application is rejected). Destroy 3 year after cutoff. (b) SPEC-accepted applications. AUTHORIZED DISPOSITION Cut off at end of calendar year (in which grant program period ends). Retire to Records Center 1 year after cutoff. Destroy 6 years, 3 months after cutoff.

## **SA&A OR ASCA**

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

Yes

*What date was it completed?*

1/27/2010



*Describe 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 (SA&A) -(Certification & Accreditation (C&A) at the time) and received an Authority To Operate (ATO) memo from Cybersecurity on 1/27/2010. As of 6/1/2010, the Security Program Management Office (SPMO) reclassified the SPECTRM application as a non-Federal Information Security Management Act (FISMA) reportable system. 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. Also, being a non-FISMA reportable system, SPECTRM is not required to conduct periodic SA&A reviews, per the SPMO. SPECTRM application virtual Wintel servers fall under the General Support Services (GSS)-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.

## **PRIVACY TESTING**

*Does the system require a System Test Plan?*

Yes

*Is the test plan completed?*

Yes

*Where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)?*

The SPECTRM application test plan is stored in both the IT-Application Development (IT-AD) Field Applications DocIT folder and the project Enterprise Life Cycle (ELC) SharePoint project folder.

*Were all the Privacy Requirements successfully tested?*

Yes

*Are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved?*

Yes

*Please describe the outstanding issues:*

Currently POAM 47254 and Work Request 860157 (with IT-D) are in place to address Guardium DB scan identified issues. Currently no Tenable, 508/IRAP, AppScan or SPLUNK issues identified.

*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?*

AppScan Enterprise for code vulnerabilities Scans 508 Testing using standard test plan, validated by IRAP Tenable Scans Guardium DB Scans SPLUNK audit logs review

## **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: Not Applicable

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?*

No