

NOTE: The following reflects the information entered in the PIAMS Website.

---

## A. SYSTEM DESCRIPTION

---

Authority: Office of Management Budget (OMB) Memorandum (M) 03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 & PVR #10- Privacy Accountability and #21-Privacy Risk Management

---

Date of Approval: 08/14/2014 PIA ID Number: 1019

---

1. What type of system is this? Non-Major System

1a. Is this a Federal Information Security Management Act (FISMA) reportable system? No

---

2. Full System Name, Acronym, and Release/Milestone (if appropriate):

Stakeholder Partnerships, Education & Communication Total Relationship Management, SPECTRM

---

2a. Has the name of the system changed? No

If yes, please state the previous system name, acronym, and release/milestone (if appropriate):

---

3. Identify how many individuals the system contains information on

Number of Employees: Under 50,000

Number of Contractors: Not Applicable

Members of the Public: Under 100,000

---

4. Responsible Parties:

NA

---

5. General Business Purpose of System

---

Stakeholder, Partnerships, Education & Communication 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 LAN in approximately 95 IRS offices or via ERAP from remote off-site locations.

6. Has a PIA for this system, application, or database been submitted previously to the Office of Privacy Compliance? (If you do not know, please contact \*Privacy and request a search) Yes

6a. If Yes, please indicate the date the latest PIA was approved: 10/15/2010

---

6b. If Yes, please indicate which of the following changes occurred to require this update.

- System Change (1 or more of the 9 examples listed in OMB 03-22 applies) (refer to PIA Training Reference Guide for the list of system changes) No
  - System is undergoing Security Assessment and Authorization No
- 

6c. State any changes that have occurred to the system since the last PIA

The Privacy Impact Assessment (PIA) for the Stakeholder Partnerships, Education & Communication Total Relationship Management (SPECTRM) system, per the PIA office, is beyond the three-year expiration period and must be updated. Per the Privacy Office communication, PIAs must be updated every 3 years. This submission is to comply with that requirement for SPECTRM.

---

7. If this system has an Exhibit 53 or Exhibit 300 please provide the Unique Project Identifier (UPI) number (XXX-XX-XX-XX-XX-XXXX-XX). Otherwise, enter the word 'none' or 'NA'. NA

---

## B. DATA CATEGORIZATION

---

Authority: OMB M 03-22 & PVR #23- PII Management

8. Does this system collect, display, store, maintain or disseminate Personally Identifiable Information (PII)? Yes

8a. If No, what types of information does the system collect, display, store, maintain or disseminate?

9. Indicate the category that best describes the source that provides or originates the PII collected, displayed, stored, maintained or disseminated by this system. Most common categories follow:

Taxpayers/Public/Tax Systems No

Employees/Personnel/HR Systems Yes

Other Yes

*Other Source:*

Volunteers (VITA/TCE Program)

10. Indicate all of the types of PII collected, displayed, stored, maintained or disseminated by this system. Then state if the PII collected is on the Public and/or Employees. Most common fields follow:

TYPE OF PII	Collected?	On Public?	On IRS Employees or Contractors?
Name	Yes	Yes	Yes
Social Security Number (SSN)	No	No	No
Tax Payer ID Number (TIN)	No	No	No
Address	Yes	Yes	No
Date of Birth	No	No	No

Additional Types of PII: Yes

<u>PII Name</u>	<u>On Public?</u>	<u>On Employee?</u>
Phone Number	Yes	No
E-mail	Yes	No

10a. Briefly describe the PII available in the system referred to in question 10 above.

VITA/TCE Partnering volunteers submit their name, address, phone number, and e-mail address, and partnering organization name via form 13615 Volunteer Standards of Conduct Agreement – VITA/TCE Programs.

If you answered Yes to Social Security Number (SSN) in question 10, answer 10b, 10c, and 10d.

10b. Cite the authority that allows this system to contain SSN's? (e.g. specific regulations, statutes, etc.)

10c. What alternative solution to the use of the SSN has/or will be applied to this system? (e.g. masking, truncation, alternative identifier)

10d. Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of Social Security Numbers on this system?

11. Describe in detail the system's Audit Trail. State what data elements and fields are collected. Include employee log-in information. If the system does not have Audit capabilities, explain why an Audit Trail is not needed.

SPECTRM records user logins via a last access date field in the user table, authenticating against the user's LAN SEID, inheriting authentication from the user's LAN login. Created Date and Created SEID, Last Update Date and Last Update SEIDs are recorded for all data changes. Transactions logs are backed up overnight and can be reviewed to identify all transactions executed by users. Standard SQL Server trace logs are also in place.

11a. Does the audit trail contain the audit trail elements as required in current IRM 10.8.3 Audit Logging Security Standards? Yes

---

12. What are the sources of the PII in the system? Please indicate specific sources:

a. IRS files and databases: No

If Yes, the system(s) are listed below:

No System Records found.

b. Other federal agency or agencies: No

If Yes, please list the agency (or agencies) below:

c. State and local agency or agencies: No

If Yes, please list the agency (or agencies) below:

d. Third party sources: Yes

If yes, the third party sources that were used are:

Non-profit partnering organizations submit information on their volunteers via form 13615 and 13206 (or spreadsheet equivalents). Volunteer information required to be in SPECTRM is input from these forms W&I CARE SPEC Tax Consultants.

e. Taxpayers (such as the 1040): No

f. Employees (such as the I-9): No

g. Other: No If Yes, specify:

---

### C. PURPOSE OF COLLECTION

Authorities: OMB M 03-22 & Internal Revenue Manual (IRM) 10.8.8, IT Security, Live Data Protection Policy & PVR #16, Acceptable Use

13. What is the business need for the collection of PII in this system? Be specific.

Non-profit partnering organizations work with IRS under the Volunteer Income Tax Assistance (VITA) and Tax Counseling for the Elderly (TCE) programs administered by W&I CARE SPEC. SPECTRM maintains basic contact information for the following individuals: Primary Contacts for Partnering Organizations; Primary Contacts and Site Coordinators for VITA/TCE free tax preparation sites; Partner volunteers receiving loaned computer equipment under VITA/TCE programs; Partnering volunteers receiving tax preparation software under the VITA/TCE programs.

---

### D. PII USAGE

Authority: OMB M 03-22 & PVR #16, Acceptable Use

14. What is the specific use(s) of the PII?

To conduct Tax Administration	<u>No</u>
To provide Taxpayer Services	<u>No</u>
To collect Demographic Data	<u>No</u>
For employee purposes	<u>No</u>

*If other, what is the use?*

Other:

Yes

To provide Points of  
Contact (POCs) for  
VITA/TCE program  
operations

---

---

**E. INFORMATION DISSEMINATION**

---

Authority: OMB M 03-22 & PVR #14- Privacy Notice and #19- Authorizations

15. Will the information be shared outside the IRS? (for purposes such as computer matching, statistical purposes, etc.) No

15a. If yes, with whom will the information be shared? The specific parties are listed below:

	Yes/No	Who?	ISA OR MOU**?
Other federal agency (-ies)			
State and local agency (-ies)			
Third party sources			
Other:			

\*\* Inter-agency agreement (ISA) or Memorandum of Understanding (MOU)

16. Does this system host a website for purposes of interacting with the public? No

17. Does the website use any means to track visitors' activity on the Internet?

If yes, please indicate means:

	YES/NO	AUTHORITY
Persistent Cookies	_____	_____
Web Beacons	_____	_____
Session Cookies	_____	_____
Other:	_____	_____

*If other, specify:*

---

**F. INDIVIDUAL CONSENT**

---

Authority: OMB M 03-22 & PVR #15- Consent and #18- Individual Rights

18. Do individuals have the opportunity to decline to provide information or to consent to particular uses of the information? Yes

18a. If Yes, how is their permission granted?

Form 13615 Volunteer Standards of Conduct Agreement – VITA/TCE Programs

19. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action? Yes

19a. If Yes, how does the system ensure "due process"?

The system will allow affective parties the opportunity to clarify or dispute negative information that could be used against them. Due process is provided pursuant to 5 USC.

20. Did any of the PII provided to this system originate from any IRS issued forms? Yes

20a. If Yes, please provide the corresponding form(s) number and name of the form.

No forms found.

20b. If No, how was consent granted?

Written consent	_____
Website Opt In or Out option	_____
Published System of Records Notice in the Federal Register	_____
Other:	_____

---

**G. INFORMATION PROTECTIONS**

---

Authority: OMB M 03-22 & PVR #9- Privacy as Part of the Development Life Cycle, #11- Privacy Assurance, #12- Privacy Education and Training, #17- PII Data Quality, #20- Safeguards and #22- Security Measures

---

**21. Identify the owner and operator of the system:** IRS Owned and Operated

**21a. If Contractor operated, has the business unit provided appropriate notification to execute the annual security review of the contractors, when required?**

---

**22. The following people have use of the system with the level of access specified:**

	<b>Yes/No</b>	<b>Access Level</b>
IRS Employees:	<u>Yes</u>	
Users		<u>Read Write</u>
Managers		<u>Read Write</u>
System Administrators		<u>Read Write</u>
Developers		<u>No Access</u>
Contractors:	<u>No</u>	
Contractor Users		<u></u>
Contractor System Administrators		<u></u>
Contractor Developers		<u></u>
Other:	<u>No</u>	<u></u>

**If you answered yes to contractors, please answer 22a.** (All contractor/contractor employees must hold at minimum, a "Moderate Risk" Background Investigation if they have access to IRS owned SBU/PII data.)

---

**22a. If the contractors or contractor employees act as System Administrators or have "Root Access", does that person hold a properly adjudicated "High Level" background investigation?**

**23. How is access to the PII determined and by whom?**

Access determination is developed at SPEC Headquarters based on the need to know. Systems and application administrators will provide access permissions via directions from SPEC Headquarters. All users requesting access to an IRS system must do so through the OL5081 process. Users are required to complete an OL5081, Information System User Registration/Change Request, which lists mandatory rules for users of IRS information and information systems. When a user has been approved for access to the SPECTRM application by his/her manager and by the HQ SPECTRM program administrator, the OL5081 system sends an e-mail to the user, providing an approval notification. Once approval has been granted, access is restricted to individuals based on their permissions, roles, scope of system access. The SEID/authentication process restricts user access to the data they are authorized to access. Contractors are not granted access to this application.

---

**24. How will each data element of SBU/PII be verified for accuracy, timeliness, and completeness?**

Data is collected on the paper forms and is reviewed and verified with the source at the SPEC territory level by the SPEC relationship manager prior to input. Also, record level business rules are performed by the system at input, providing warning of incomplete records.

---

**25. 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

---

**25a. 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.**

Data is eliminated as per IRM 1.15.57-1(1) General Records Schedule (GRS) for Electronic Records and IRM 1.15.3.2.1 Disposition of Records

**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 unclassified. 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 (NARA), 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.

---

**26. Describe how the PII data in this system is secured, including appropriate administrative and technical controls utilized.**

Access to the SPECTRM manage using multiple layers. Approved OL5081 request place 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 on the geographic scope of their SPEC Territory for field employees, Area for Area Analysts (READ ONLY), or HQ for SPEC Headquarters staff (READ ONLY). Change/Read/Update/Delete (CRUD) 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. SPECTRM records via data fields and the database transaction log which user has executed any CRUD function.

**26a. Next, explain how the data is protected in the system at rest, in flight, or in transition.**

SPECTRM is a web-based application using a C#.NET user interface and a SQL Server database. SPECTRM is only accessible by authorized users within the IRS firewall, and is not externally accessible. The application resides on Wintel virtual servers housed at IRS Enterprise Computing Centers (ECCs). Data is never in flight or in transition outside the IRS LAN environment behind the IRS LAN firewall.

---

**27. Has a risk assessment (e.g., SA&A) been conducted on the system to ensure that appropriate security controls have been identified and implemented to protect against known risks to the confidentiality, integrity and availability of the PII? Yes**

---

**28. Describe the monitoring/evaluating activities undertaken on a regular basis to ensure that controls continue to work properly in safeguarding the PII.**

SPECTRM was developed in house by IT-Application Development (IT-AD). During the development ELC process, SPECTRM was evaluated under an SA&A (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-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 HQ annually recertifies user access to SPECTRM through the OL5081 system. SPECTRM application virtual wintel servers fall under the 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.

---

**29. Is testing performed, in accordance with Internal Revenue Manual (IRM) 10.8.8 - IT Security, Live Data Protection Policy? Not Applicable**

---

**29a. Has approval been received from the Office of Privacy Compliance to use Live Data in testing (if appropriate)?**

**29b. If you have received permission from the Office of Privacy Compliance to use Live Data, when was the approval granted?**

---

**H. PRIVACY ACT & SYSTEM OF RECORDS**

Under the statute, any employee who knowingly and willfully maintains a system of records without meeting the Privacy Act notice requirements is guilty of a misdemeanor and may be fined up to \$5000.

*Authority: OMB M 03-22 & Privacy Act, 5 U.S.C. 552a (e) (4) & PVR #13-Transparency*

---

**30. Are 10 or more records containing PII maintained/stored/transmitted through this system? Yes**

---

31. Are records on the system retrieved by any identifier for an individual? (Examples of identifiers include but are not limited to Name, SSN, Photograph, IP Address) Yes

31a. If YES, the System of Records Notice(s) (SORN) published in the Federal Register adequately describes the records as required by the Privacy Act? Enter the SORN number and the complete name of the SORN.

**SORNS Number**

**SORNS Name**

10.004	Stakeholder Relationship Management and Subject Fi
34.037	The IRS Audit Trail and Security Records System
36.003	General Personnel and Payroll Records
22.062	Electronic Filing Records
10.007	SPEC Taxpayer Asst Rpt Sys (now SPECTRM)

**Comments**

## I. ANALYSIS

---

Authority: OMB M 03-22 & PVR #21- Privacy Risk Management

---

**32. What choices were made or actions taken regarding this IT system or collection of information as a result of preparing the PIA?**

Resulted in the removal of PII from the system (e.g., SSN use reduced/eliminated)	<u>No</u>
Provided viable alternatives to the use of PII within the system	<u>No</u>
New privacy measures have been considered/implemented	<u>No</u>
Other:	<u>No</u>

**32a. If Yes to any of the above, please describe:**

Not Applicable

[View other PIAs on IRS.gov](#)