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: 01/31/2014 PIA ID Number: **755**

1. What type of system is this? New

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

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

Telework for Customer Service Representatives (CSRs) Pilot, none

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:	Not Applicable
Number of Contractors:	Not Applicable
Members of the Public:	Not Applicable

4. Responsible Parties:

NA

5. General Business Purpose of System

The Telework for CSRs Pilot is a viable option to mitigate Accounts Management future staffing and seating capacity needs. CSRs will work from a remote location (home environment) and complete the same job responsibilities as they would in an IRS brick and mortar location; responding to customer telephone inquiries on tax law, procedural, and account issues, and working elecronic inventory through the Correspondence Imagery System (CIS). One of the key drivers behind Telework for CSRs is the need to expand our staffing and seating capacity without increasing our real estate footprint. Telework will bring direct and indirect benefits to AM such as a more engaged workforce, continuities of operations during emergencies and closures, and scheduling efficiencies; as well as support the IRS "Best Place to Work" goal. Telework provides employees greater flexibility in balancing their work and family responsibilities. Findings show that employees participating in Telework use less leave, have lower commuting costs, are more productive, and engage in technology to its fullest extent. The Telework for CSRs pilot will initially involve 56 agents (CSRs and Managers; 2 teams with a SOC of 13:1 each; from 2 sites, a remote and a campus). The pilot will have a phased expansion to include a total of 224 agents (12 teams at 4 sites). Telework for CSRs follows existing IRM procedures and the National Agreement, Articles 11 and 50. Participation is voluntary and selections would be made by EOD. CSR Teleworkers would work from home four days per week. On the days they report to the office, they will sit in designated work stations that will be shared on a 3:1 basis. When those designated work stations are not being used by Teleworkers, they will be used for hoteling. Title 26 provisions provide due process for taxpayers.

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*) No

6a. If Yes, please indicate the date the latest PIA was approved:

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)**
- **System is undergoing Security Assessment and Authorization**

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

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	Yes	
Employees/Personnel/HR Systems	No	
		Other Source:
Other	No	

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)	Yes	Yes	No
Tax Payer ID Number (TIN)	Yes	Yes	No
Address	Yes	Yes	No
Date of Birth	Yes	Yes	No

Additional Types of PII: No

PII Name	On Public?	On Employee?
	No	No

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

CSRs that Telework will be able to access the IDRS/CFOL and AMS systems through ERAP, in response to a customer account related inquiry. These systems display all entity and account information for the primary person listed on the account. This includes the the PII listed above, as well as income information from payers, employer information and banking information. In addition, the primary account information may contain spouse's name and identification number, dependent's name and identification number, and other finanacial information.

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.)

Internal Revenue Code 6109

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

NA

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

NA

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.

We are not creating new audit trails for the systems that technicians will be accessing. The current audit trails for the existing systems, such as IDRS, CFOL, AMS, etc., used by CSRs in an IRS brick and mortar facility will continue to be in effect for the CSR that Teleworks. Telework, in and of itself, does not have an audit trail.

11a. Does the audit trail contain the audit trail elements as required in current IRM 10.8.3 *Audit Logging Security Standards*? No

---

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

a. IRS files and databases: Yes

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: No

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

e. Taxpayers (such as the 1040): Yes

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.

The objective for the Telework for CSRs Pilot is to maintain or improve employee and customer satisfaction, while gaining efficiencies in cost savings and productivity. The CSR workforce will need to expand to handle additional toll-free telephone demand and electronic CIS inventory. Telework provides that capability without increasing the IRS space footprint and the associated rent and facility costs. During the Telework for CSRs Pilot, the CSR will be accessing account information through IDRS/CFOL and AMS in response to a customer telephone inquiry or an electronic inventory case resulting from taxpayer correspondence. The account information will be displayed to the CSR in the remote, home location in the same manner as it is displayed in an IRS brick and mortar facility.

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	Yes	
To provide Taxpayer Services	Yes	
To collect Demographic Data	No	
For employee purposes	No	
		If other, what is the use?
Other:	No	

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? Not Applicable

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

19. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action? Not Applicable

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

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:

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

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?

The ability to access PII is defined by the position description of the Customer Serveice Representative and the Supervisory Cutomer Service Representative, and access to systems displaying the PII is approved through the on line 5081 process.

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

When responding to a customer account inquiry, the CSR is required to complete taxpayer authentication before disclosing any account information. Procedures for required disclosure probes are covered in IRM 21.1.3.2.3, and apply whether the CSR is Teleworking or working from an IRS brick and mortar facility.

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? Yes

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.

Managers will perform reviews of employees and maintain performance files in the same manner regardless of whether an employee Teleworks or works from a IRS brick and mortar facility. The records related to performance reviews are maintained in the Embedded Quality Review System (EQRS), which has a separate PIA and data disposition instructions, as approved under National Archives Job No. N1-58-12-16. EQRS data is approved for destruction 5 years after the close of the reporting year. This will be published in IRS Document 12990, Records Control Schedule 31 for Customer Service, item 10(2), when next updated. Employees will not be required to maintain records at their homes since all the relevant databses or systems they will use are electronic.

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.

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

Customer account data displayed through the IDRS system is secured through ERAP in the current Telework environment. A Service Wide Voice/Data Encryption Solution through ERAP should be availabe in September, 2014, that will enable account related telephone calls that require taxpayer authentication to be routed to the Telework CSR. According to the 2012 National Agreement, Article 50, in order to be eligible to participate in Telework, the employee must have a "work space suitable to perfrom work, utilities adequate for installing equipment, and a general work environment that is free from interruptions and provides reasonable security and protection for government property. A successful Telework program is dependent on the participating employees being overly cautious of adhering to the physical and cyber security requirements (IRMs 6.800 and 1.16). The employee is held accountable for following those requirements; however, the manager takes action only when a complaint is received. Per Article 50, Setion 4(D), Management has the right to conduct on-site visits to ensure Information Systems and sensitive information procedures are in place. Revenue Agents and Revenue Officers that currently Telework are able to access taxpayer account data on IDRS without violating physical and cyber security requirements. The Telework employee is required to sign a form that is retained by the manager that s/he reviews and becomes familiar with the content in the home office safety handbook.

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

Telework participants must be mindful of adhering to the physical and cyber security requirements, just as if they were in an IRS on site location. Article 50, Section 5 discusses the employee's responsibilities while Teleworking: "B. Employees must protect all Government records and data against unauthorized disclosure, access, mutilation, obliteration, and destruction. Files and other information that are subject to the Privacy Act regulations must be secured in a way that renders these records and data inaccessible to anyone other that the employee. At a minimum, this will require that all records and data be kept under lock and key when not in the possession of the employee. C. Employees must comply with all required security measures and disclosure provisions, including password protection and data encryption so that at no time are the security, disclosure, or Privacy Act requirements of the Service compromised. D. Employees must ensure that government provided equipment/property is used only for authorized purposes. Telework participants will be provded with a lap top computer equipped with a channel lock. Participants must follow the security guidelines for transporting a lap top computer when going to and from the office location.

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? No

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

Monitoring and evaluating activities to ensure the safeguarding of the PII would be the same for the Telework participant as the CSR working in an IRS office. The same security and systems reports are run to monitor safeguarding of PII regardless of the physical location where the work is performed. Per the contract, Management has the right to conduct on-site visits of the remote location to ensure that Information Systems and sensitive procedures are in place. Telework participants will be provided with a web cam that could also be used as a method of spot checking the home work environment without having to conduct an actual on site visit.

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
Treas/IRS 00.001	Correspondence
Treas/IRS 24.030	IMF
Treas/IRS 24.046	BMF
Treas/IRS 34.037	IRS Audit Trail and Security Records System

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)	No
Provided viable alternatives to the use of PII within the system	No
New privacy measures have been considered/implemented	No
Other:	No

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

Not Applicable

View other PIAs on IRS.gov