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: Aug 26 2013 12:00AM PIA ID Number: **587**

1. What type of system is this? Major System

1a. Is this a Federal Information Security Management Act (FISMA) reportable system? Yes

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

Enterprise Convergence, Convergence

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:	More than 100,000
Number of Contractors:	Over 10,000
Members of the Public:	Over 1,000,000

4. Responsible Parties:

NA

5. General Business Purpose of System

IRS voice, video, data, and fax services are currently transported across disparate, isolated networks using diverse hardware and software technologies. Specifically, voice is transported via separate voice networks, such as the Public Switched Telephone Network (PSTN); video is transported across separate circuits between IRS locations, and data is transported over wide area networks (WAN) and local area networks (LAN). Moreover, voicemail systems utilize another separate set of circuits and infrastructure elements. Consequently, IRS offices require site-unique implementations resulting in a lack of technical standardization and the need for additional operational support and resources. The Network Convergence Project was established to address these issues as well as refresh end of life telephony and video technology. Network Convergence supports the following capabilities: • Unified Messaging. Integration of multiple Voice Over Internet Protocol (VoIP) technologies, such as telephony, electronic mail, instant messaging, and video. • Call History. Logs of placed, received, and missed calls on all devices. • Extension Mobility. Ability to log into any Convergence-enabled IP Desk Phone regardless of location within the Enterprise. • Soft Phone Technology. A software application that provides full-featured VoIP telephony services. • ViewMail Integration. An extension to the Microsoft Outlook application that enables receipt, processing, and management of VoiceMail messages. Key improvements to be realized as a result of Network Convergence include: • Centralization of enterprise call control, processing services, and emergency response (E911) • Consolidation of local and long distance access lines • Utilization of the Treasury wide area network (TNET) as a surrogate for transporting Voice over Internet Protocol (VoIP) and Video • Integration of various electronic messaging and communications media into a common interface accessible from a variety of different devices, e.g., Unified Messaging. Integrated media included but are not limited to electronic mail, instant messaging, facsimile transmissions, voicemail, and video messaging • Modernization and refresh upgrades for routers, switches, and infrastructure cabling at Converged sites.

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: __/__/____

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) Yes
- System is undergoing Security Assessment and Authorization

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

1) The ViewMail privacy issue associated with the Microsoft Outlook application displaying the Caller Name and Phone Number in the Subject Line of the message when a call has been missed and/or a Voicemail message has been left for the User has been resolved. Caller PII is no longer displayed. 2) The e911 RedSky privacy issue associated with retention of employee personal information in the RedSky cloud database is no longer applicable. IRS personnel working remotely have been advised not to use their soft phones for Emergency Responder services. Moreover, the e911 RedSky application needed to support 911 services will not be purchased for use outside of the IRS network. 3) The use of .WAV files for storing voice mail messages has been introduced to meet unique Treasury Inspector General for Tax Administration (TIGTA) and IRS Criminal Investigations (CI) requirements.

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 Yes

Other No

Other Source:

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

Additional Types of PII: Yes

PII Name	On Public?	On Employee?
Individual Phone Number	Yes	Yes

10a. What is the business purpose for collecting and using the SSN ?

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?

Describe the PII available in the system referred to in question 10 above.

An IRS Privacy Impact Assessment – Qualifying Questionnaire, for the Convergence Pilot was submitted on February 8, 2012. At that time it was indicated the Convergence Pilot did not process private and sensitive information, as defined in The Privacy Act of 1974. However, the current Enterprise-wide Network Convergence effort has revealed three key elements that may have Privacy-related implications. Specifically: • Cisco IP Desk Phone Directory. Displays the caller name and phone number in a directory of received, missed, and placed calls. This capability exists in many of the current telephone configurations. The primary issue is the retention of this information on the device and the ease of access to unauthorized/unauthenticated individuals. Technical solutions exist for removing this display but will eliminate key user functionality. • Cisco IP Desk Phone Assigned Keys. The Cisco IP Desk Phone enables users to assign a limited number of keys to specific phone numbers to facilitate quickly placing calls. The user can enter a unique name and phone number and assign it to one of the "hot keys". The name and phone number are presented on the display screen. The primary issue is the retention of this information on the device and the ease of access to unauthorized/unauthenticated individuals. Technical solutions exist for removing this display but will eliminate key user functionality. • .WAV File Storage and Transmission. On a special needs and request basis, TIGTA special agents will be able to receive and retain voicemail (audio) messages in the form of .WAV files to be used as evidence in follow-up actions stemming from verbal threats to themselves or the organization that have been received on their voicemail system. In special cases, the TIGTA Program will request the Convergence PMO provide a .WAV file of a specific voicemail record. A .WAV file will be generated by a Convergence System Administrator and securely transmitted to the TIGTA program office via a secure, encrypted repository established for sharing sensitive information between IRS and TIGTA. • ViewMail Application. CI personnel will receive their ViewMail voice messages as .WAV files via an Outlook Email message. • E911 Application. Network Convergence is leveraging the RedSky e911 application to facilitate emergence response services within the Enterprise for soft phone users. No Privacy-related issues exist with the Enterprise implementation of the ResSky e911 application. Outside of the Privacy-related concerns articulated above, Network Convergence is an infrastructure system that operates within the MITS-29 security boundary. It will maintain an audit trail and audit logs to be incorporated into the MITS-29 SA&A Audit Plan. Audit logging will include, but not be limited to, the following data elements: • Call detail records (CDR). To capture the called number, the number that placed the call, the date and time a call was started, the time it connected, and the time it ended. • Call management records (CMR). Diagnostic records that document jitter, lost packets, and the amount of data sent and received during the call, latency, and MOS. A single call can result in the generation of multiple CDRs and CMRs. The Network Convergence Call Manager contains a searchable directory of all personnel (IRS employees and contractors) assigned a phone number. It is searchable using an individual’s First Name, Last Name, or phone extension. The data populated into the directory is acquired from Active Directory and is the same source used to support the IRS Microsoft Outlook email system. Network Convergence VoIP traffic is securely transmitted over the WAN via TNET using IPSec encrypted tunnels managed and maintained by the vendor, AT&T. As such, there is a potential that AT&T personnel with access to these routers could intercept traffic before it is encrypted thus giving them access to voice conversations or voice mail traffic where intercepted calls may contain PII information related to taxpayers or employees. IRS has no control of voice conversations as they exit the IRS network to the Public Switch Telephone Network (PSTN) and are not able to perform end to end encryption of calls that leave the IRS network. Therefore, there is no expectation of privacy for any calls that do not remain within the IRS network.

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.

Outside of the Privacy-related concerns articulated above, Network Convergence is an infrastructure system that operates within the MITS-29 security boundary. It will maintain an audit trail and audit logs to be incorporated into the MITS-29 SA&A Audit Plan. Audit logging will include, but not be limited to, the following data elements: • Call detail records (CDR). To capture the called number, the number that placed the call, the date and time a call was started, the time it connected, and the time it ended. • Call management records (CMR). Diagnostic records that document jitter, lost packets, and the amount of data sent and received during the call, latency, and MOS. A single call can result in the generation of multiple CDRs and CMRs. The Network Convergence Call Manager contains a searchable directory of all personnel (IRS employees and contractors) assigned a phone number. It is searchable using an individual’s First Name, Last Name, or phone extension. The data populated into the directory is acquired from Active Directory and is the same source used to support the IRS Microsoft Outlook email system. Network Convergence VoIP traffic is securely transmitted over the WAN via TNET using IPSec encrypted tunnels managed and maintained by the vendor, AT&T. As such, there is a potential that AT&T personnel with access to these routers could intercept traffic before it is encrypted thus giving them access to voice conversations or voice mail traffic where intercepted calls may contain PII information related to taxpayers or employees. IRS has no control of voice conversations as they exit the IRS network to the Public Switch Telephone Network (PSTN) and are not able to perform end to end encryption of calls that leave the IRS network. Therefore, there is no expectation of privacy for any calls that do not remain within the IRS network.

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: No

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

e. Taxpayers (such as the 1040): No

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

g. Other: Yes If **Yes**, *specify*: Name and phone number are gathered as a result of phone calls made, received, or missed.

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.

1) IP Desk Phone - Call log containing Caller Name and Number provides a searchable history of made, received, and missed calls on the IP Desk Phone. This is only accessible on the specific IP Desk Phone. 2) ViewMail - After missing a call an email is sent to the recipient's IRS Email account and displays the Caller's Name and Phone Number in the EMail Subject Line. Only internal caller information is displayed in the Subject Line. External caller information is not transmitted or presented in the Subject Line of the Email Message. 3) TIGTA .WAV Files - Collected voicemail records will be used for audit activities upon special request. 4) CI .WAV Files - Collected voicemail messages will be received by all CI personnel to support investigative actions.

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	No	
To provide taxpayer services	No	
To collect demographic data	No	
For employee purposes	Yes	
		If other, what is the use?
Other:	Yes	1) IP Desk Phone - Call History, 2) ViewMail - track missed calls2) TIGTA .WAV files - Special case audit scenarios, as required and requested3) CI .WAV files - Investigative actions.

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		

If other, specify:

Other: ____________ ____________________

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?

Individuals do not need to leave voice messages in the system.

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? No

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	No
Website Opt In or Out option	No
Published System of Records Notice in the Federal Register	No
Other:	No

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 Contractor 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		No Access
System Administrators		Read Write
Developers		No Access
Contractors:	Yes	
Contractor Users		Read Write
Contractor System Administrators		Read Write

Contractor Developers		No Access
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? Yes

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

1) IP Desk Phone - Anyone with access to the IP Desk Phone may select the directory option and review the Call History to include Name and Phone Number for calls made, calls received, and calls missed. Assigned "hot keys" may display personally identifiable information entered by the user. 2) TIGTA .WAV files - Requested voice mail .WAV files will be transmitted to the TIGTA secure server for retrieval. TIGTA special agents will be responsible for their storage, processing, retention, security, and ultimate disposition. 3) CI .WAV files - All CI personnel will receive their voicemail messages in the ViewMail application as .WAV files. CI Personnel will be responsible for their storage, processing, retention, security, and ultimate disposition.

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

The data collected is derived and passed from the telephone systems in use. It is not verified for accuracy, timeliness, or completeness.

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.

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.

Network Convergence is non-recordkeeping, and does not require National Archives and Records Administration approval for records disposition or retention. As operated within the IT/MITS-29 (General Support System, GSS-29 security/infrastructure support domain) it consolidates and centralizes a variety of diverse hardware and software technologies that support IRS phone, video and electronic messaging and communications. Audit logs are maintained in accordance with General Records Schedule (GRS) 20, Item 1c (published in IRS Document 12829) and will be deleted/destroyed when they are no longer needed for administrative, legal, audit, or other operational purposes. In general, records will be retained for a minimum of 90 days. TIGTA compliance may require retention up to 7 years in duration. See below for specific circumstances: 1) IP Desk Phone - Records are maintained at the device and will be cleared as they are willfully deleted or space limitations require deletion of historical data. 2) Viewmail - Retained for 14 days.

26. Describe how the PII data in this system is secured, including appropriate administrative and technical controls utilized.
1) IP Desk Phone - Devices are physically secured in IRS facilities. The user-entered "hot key" phone contact information and the call history data, e.g., calls made, calls received, and calls missed can only be accessed physically via the actual hard IP desk phone device. The call history data cannot be accessed received, or transmitted logically via the IRS computer network. 2) ViewMail - Email messages containing missed phone call data are stored in the users Inbox and can only be accessed by users that have logged onto their account via the standard login process. MS Outlook email messages are stored in accordance with overarching IRS Microsoft Outlook security requirements. Users are prohibited per IRS Policy from forwarding emails with PII. 3) .WAV files - .WAV files are a data file containing an audio recording and may be stored and transmitted in the manner as any other file. TIGTA .WAV files will be transmitted to the TIGTA secure server by Convergence System Administrators and retrieved by the requesting TIGTA Special Agent. The Special Agent may store and transmit the file as normal. CI .WAV files are stored securely in the Microsoft Outlook database. These files may be retrieved, stored and transmitted in the same manner as any other file.

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

1) IP Desk Phone - Devices are physically secured in IRS facilities. The user-entered "hot key" phone contact information and the call history data, e.g., calls made, calls received, and calls missed can only be accessed physically via the actual hard IP desk phone device. The call history data cannot be accessed received, or transmitted logically via the IRS computer network. 2) ViewMail - All VoIP Traffic is encrypted using various technical protocols operating on the TNET, e.g., SRTP, etc., using FIPS 140-2 compliant encryption technologies. 3) Voice Mail Messages - All CI .WAV files are centrally and securely stored on the Microsoft Outlook server. Downloaded TIGTA .WAV files are transmitted to a secure server for retrieval. All .WAV files may be stored and transmitted, in a manner similar to any other data file.

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.

Network Convergence is a sub-element of the Common Premise Capability, Voice Messaging System, and Videoconferencing System components of GSS-29. The monitoring and evaluation controls are inherited from GSS-29.

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**
trea/irs 34.037	IRS audit log and security records system
Treas/IRS 00.001	Correspondence Files and Correspondence Control Fi

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	Yes
Other:	No

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

The display of external phone caller PII (Name and Phone Number) on the IP Desk Phone when receiving a call has been specifically removed through reconfigured administrative settings.