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: 03/19/2014 PIA ID Number: **805**

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):

Convergence Jabber/WebEx, Convergence Jabber/WebEx

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

The Network Convergence Project (see PIA # 359) was established to refresh end of life telephony and video technology.

It 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 integrated into the Microsoft Office Communication System (OCS) that provides full-featured VoIP telephone services.
- ViewMail Integration. An extension to the Microsoft Outlook application that enables receipt, processing, and management of VoiceMail messages. This PIA addresses related Cisco Network technologies being Piloted for possible introduction into the Network Convergence System:
- Cisco Jabber - a potential replacement softphone application for the CUCILYNC softphone application currently in use. Cisco Jabber streamlines communications and enhances productivity by unifying presence, instant messaging, video, voice, voice messaging, desktop sharing, and conferencing capabilities securely into one client on the IRS user's desktop.
- WebEx - A potential replacement for the current LiveMeeting application used by IRS personnnel for Internal Video-based meetings.

  Web-Ex will be available in two forms as follows: 1) WebEx Meeting Center on premise (OnPrem). enabling encrypted voice and video communications within the IRS enterprise for IRS employees for secure communications of sensitive, but unclassified (SBU) data. 2) WebEx Meeting Center in the Cloud. Scales to accommodate more participants outside of the IRS network but is limited to displaying non-SBU information only. Due process is provided applicable to the kind of information pursuant to 26 USC or 5 USC .

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)** 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 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)	No	No	No
Tax Payer ID Number (TIN)	No	Yes	No
Address	No	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. Briefly describe the PII available in the system referred to in question 10 above.

The PII elements can include any information associated with the Public, IRS employees, or IRS contractors. Jabber, WebEx OnPrem, and WebEx Cloud are not specifically used to collect, generate, store, or maintain PII. However, these audiovisual applications may be used to display or disseminate PII aurally or via online display mechanisms as described below. PII information can be disseminated as follows: Jabber 1) Internal to IRS telephone network – PII may be transmitted via telephone discussion (audio), via teleconference discussion (audio), via videoconference (audio and display), via file transmission (files and data) 2) External to IRS telephone network – PII may be transmitted via telephone discussion (audio) and via teleconference discussion (audio) WebEx OnPrem – Internal to IRS Network – PII may be transmitted via web conference (audio, interactive display, and file sharing) involving IRS personnel (Employees and Contractors) with valid network credentials. WebEx Cloud – External to IRS Network – PII may be transmitted via web conference (audio only) involving IRS personnel (Employees and Contractors) with valid network credentials and members of the public with valid Cisco WebEx cloud credentials.

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.

See the Convergence PIA #359 for information regarding audit logs for telephone calls. The Jabber application maintains the complete dialogue of all instant messages for an individual and their contacts. A log of phone calls is also maintained. The WebEx OnPrem and Cloud implementations do not collect or maintain specific PII other than caller credentials. Specifically, external participants register their login id (email address) and password information. Administration of these credentials are handled by Cisco System Administrators operating using secure application environments.

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: No **If Yes*, specify*:** input data here

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.

Information collected during Jabber, WebEx OnPrem, and WebEx Cloud sessions are discussed and presented in support of the IRS mission. For all intents and purposes the Jabber and WebEx applications are transport mechanisms and not actual storage containers. For example PII may be discussed internally via a Jabber phone call, displayed during a Jabber video session, transmitted in an instant message, or transferred in a file. PII may be discussed externally via a Jabber phone call. Similarly, PII may be discussed internally via a teleconference, displayed during an intereactive videoconference, or transferred in a file. PII may also be discussed externally via a teleconference with authenticated and authorized personnel

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	PII is used in support of the IRS mission. The nature of its use is strictly to support the general business needs of IRS personnel. In this capacity, the Jabber, WebEx OnPrem, and WebEx Cloud are used as transport mechanisms to support interpersonal activities. Data collected is not retained or maintained for any other purposes.

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)	No		No
State and local agency (-ies)	No		No
Third party sources	No		No
Other:	No		

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

16. Does this system host a website for purposes of interacting with the public? Yes

17. Does the website use any means to track visitors' activity on the Internet? No

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?

Input data here

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?

No specific PII access determination requirements exist because PII is not specifically collected, generated, or maintained using Jabber, WebEx OnPrem, or WebEx Cloud. Instead these systems may or may not be used to discuss /convey PII as a part of normal IRS business processes when using the application.

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

There are no mechanisms for adjudicating the accuracy, timeliness or completeness of PII handled via Jabber and WebEx communications.

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.

See the Convergence PIA #359 for additional information on data retention. Essentially Jabber, WebEx OnPrem, and WebEx Cloud are non-recordkeeping systems and do not require National Archives and Records Administration approval for records disposition or retention. Audit logs are maintained in accordance with General Records Schedule (GRS) 20 - IRM 1.15.57, Item 1c 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.

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

Operational security controls in the form of IRM 10.5.1.5, Service-wide Roles and Responsibilities, apply during use of the Jabber, WebEx OnPrem, and WebEx Cloud applications for discussion of PII. The Jabber and WebEx

applications leverage TNET LAN encryption technologies to secure communications transiting the IRS network. All communications exiting the IRS network must transit the Public Switched Telephone Network (PSTN) and therefore cannot be encrypted

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

The following technical controls apply for data at rest and in transit. Jabber and WebEx OnPrem– The IRS identification, authentication, and authorization mechanism is required to access and use the Jabber and WebEx OnPrem applications. The Jabber and WebEx OnPrem applications leverage TNET LAN encryption technologies to secure communications transiting the IRS network. All communications exiting the IRS network must transit the PSTN and therefore cannot be encrypted. Individuals leveraging the WebEx Cloud application must identify and authenticate using proprietary Cisco identity management tools

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.

The Jabber and WebEx OnPrem components of Network Convergence are sub-elements 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. The WebEx Cloud is not monitored by IRS, rather it is monitored by Cisco.

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

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	Yes
Other:	No

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

tbd

View other PIAs on IRS.gov