Date of Approval: July 26, 2017 PIA ID Number: **1766**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database.
Convergence/Jabber/WebEx, CWMS

2. Is this a new system? No

2a. If **no**, is there a PIA for this system? Yes

If **yes**, enter the full name, acronym, PIA ID Number and milestone of the most recent PIA.

PIA #1275, Convergence Jabber/WebEx/CWMS, Milestone 4b

Next, enter the **date** of the most recent PIA. 5/26/2015

Indicate which of the following changes occurred to require this update (check all that apply).

No	Addition of PII
No	Conversions
No	Anonymous to Non-Anonymous
No	Significant System Management Changes
No	Significant Merging with Another System
Yes	New Access by IRS employees or Members of the Public
No	Addition of Commercial Data / Sources
Yes	New Interagency Use
No	Internal Flow or Collection

Were there other system changes not listed above? No

If yes, explain what changes were made.

3. Check the current ELC (Enterprise Life Cycle) Milestones (select all that apply)

No	Vision & Strategy/Milestone 0
No	Project Initiation/Milestone 1
No	Domain Architecture/Milestone 2
No	Preliminary Design/Milestone 3
No	Detailed Design/Milestone 4A
Yes	System Development/Milestone 4B
No	System Deployment/Milestone 5
No	Operations & Maintenance (i.e., system is currently operational)

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

A.1 General Business Purpose

5. 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.

The Network Convergence Project (see PIAs # 359, 520, 656, 1275) 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 that provides full-featured VoIP telephone services streamlining 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. • ViewMail Integration. An extension to the Microsoft Outlook application that enables receipt, processing, and management of VoiceMail messages. A key facet of the Network Convergence Project is Multi-user Conferencing Services using the Cisco WebEx Meeting Server (CWMS) application to host meetings involving IRS personnel within the IRS wide area network (WAN) boundary and external users via the Internet. CWMS connects to a proxy server in the Common Communication Gateway (CCG) to facilitate external collaboration with participants outside of the IRS network. Due process is provided for information discussed and presented pursuant to 26 USC or 5 USC. CWMS provides IRS personnel a mechanism to conduct teleconferences and web conferences with personnel within the IRS WAN and external participants via the Internet. As a result, the potential exists for sharing personally-identifiable information (PII) and sensitive but unclassified (SBU) data. During CWMS teleconferences and web conferences hosts and participants may discuss PII and SBU data in support of the IRS mission so long as IRS employees and cleared contractors adhere to all IRMs governing discussion of PII and/or SBU. The following CWMS web conference components are available for mission-related information-sharing and collaboration, to include PII and SBU data: - Share application – Any application currently opened by the presenter can be shared and displayed with CWMS web conference participants. - Share file – A file on any drive accessible to the presenter can be selected, opened, and shared with CWMS web conference participants. A CWMS user presentation interface provides the construct for displaying the file data. - White Board – The presenter may enter information directly onto the whiteboard and share it with the CWMS web conference participants. - Recording: Hosts have the ability to record CWMS web conference meetings, to include materials shared and the discussion. This information is stored centrally in the CWMS database. The Host may access and retrieve the recorded meeting via their personal WebEx Web Page. Access is secured via IRS PIV Card identification and authentication services. To limit unauthorized disclosure of PII and SBU data, the following CWMS Features are globally disabled during web conferences: - Remote Desktop Control: No meeting participant may be granted access and control of the presenter’s computer. - File Transfer: Files may not be transferred between meeting participants. - Desktop Sharing: Only Application and File sharing is permitted. Preventing desktop sharing ensures PII and SBU data are not inadvertently compromised. Detail Records are generated for CWMS teleconferences and web conferences. The following information is contained in these records which are only accessible by system administrators approved via the OL5081 application: - Participant Phone Number - Participant name (as entered by the participant attending on-line web conferences via the web). For external callers, this is not available. - System-related SBU information, such as IP addresses, used to monitor CWMS performance during teleconferences and web conferences. All BODS /Units may use this for SBU/PII and could include tax return information.

B. PII DETAIL

6. Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any type of Sensitive but Unclassified (SBU) or Personally Identifiable Information (PII)? Yes

6a. If **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.)? Yes

If **yes**, check who the SSN (or tax identification number) is collected on.

Yes On Primary Yes On Spouse Yes On Dependent

If **yes**, check all types SSN s (or tax identification numbers) that apply to this system:

Yes	Social Security Number (SSN)
Yes	Employer Identification Number (EIN)
Yes	Individual Taxpayer Identification Number (ITIN)
Yes	Taxpayer Identification Number for Pending U.S. Adoptions (ATIN)
Yes	Practitioner Tax Identification Number (PTIN)

Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of SSN s (or tax identification numbers).

The CWMS application is a web-based tool that supports teleconferencing services with individuals outside of the IRS. No specific PII data is generated or stored by the system during a CWMS session. However, the potential exists for a participant in the WebEx session to discuss PII / sensitive data. Moreover, presenters may share presentation materials and other applications / artifacts that display PII / sensitive data. Screen capture and 3rd party recording tools may be used by meeting participants to collect information shared via WebEx. To mitigate to limit unauthorized disclosure of PII and SBU data from a technical perspective, the following CWMS Features globally are disabled during web conferences: - Remote Desktop Control: No meeting participant may be granted access and control of the presenter's computer. - File Transfer: Files may not be transferred between meeting participants. - Desktop Sharing: Preventing desktop sharing ensures PII and SBU data are not inadvertently compromised. In addition to the above technical prohibitions, IRS policy specifically prohibits the sharing of PII with unauthorized personnel. Any breaches must immediately be reported in accordance with IRS Incident Reporting requirements.

6b. Does this system contain other (non-SSN) PII that it uses, collects, receives, displays, stores, maintains, or disseminates? (i.e. Names, addresses, etc.) Yes

If **yes**, specify the information.

Selected	PII Element	On Primary	On Spouse	On Dependent
Yes	Name	Yes	Yes	Yes
Yes	Mailing address	No	No	No
Yes	Phone Numbers	No	No	No
Yes	E-mail Address	No	No	No
Yes	Date of Birth	Yes	Yes	Yes
Yes	Place of Birth	No	No	No
Yes	SEID	No	No	No
Yes	Mother's Maiden Name	No	No	No
Yes	Protection Personal Identification Numbers (IP PIN)	No	No	No
Yes	Internet Protocol Address (IP Address)	No	No	No
Yes	Criminal History	No	No	No
Yes	Medical Information	No	No	No
Yes	Certificate or License Numbers	No	No	No
Yes	Vehicle Identifiers	No	No	No
Yes	Passport Number	No	No	No
Yes	Alien (A-) Number	No	No	No
Yes	Financial Account Numbers	No	No	No
Yes	Photographic Identifiers	No	No	No
Yes	Biometric Identifiers	No	No	No
Yes	Employment (HR) Information	No	No	No
Yes	Tax Account Information	Yes	Yes	Yes

6c. Does this system contain SBU information that is not PII, it uses, collects, receives, displays, stores, maintains, or disseminates? Yes

If **yes**, select the types of SBU

Selected	SBU Name	SBU Description
Yes	Agency Sensitive Information	Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission
Yes	Procurement sensitive data	Contract proposals, bids, etc.
Yes	Official Use Only (OUO) or Limited Official Use (LOU)	Information designated as OUO or LOU is information that: is exempt under one of the statutory Freedom of Information Act exemptions; is prohibited by other laws or regulations; would significantly impede the agency in carrying out a responsibility or function; or would constitute an unwarranted invasion of privacy.
Yes	Proprietary data	Business information that does not belong to the IRS
Yes	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
Yes	Physical Security Information	Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities
Yes	Criminal Investigation Information	Information concerning IRS criminal investigations or the agents conducting the investigations.

6d. Are there other types of SBU/PII used in the system? No

6e. Cite the authority for collecting SBU/PII (including SSN if relevant)

Yes	PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(a)
Yes	SSN for tax returns and return information is Internal Revenue Code Section 6109
Yes	SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397
Yes	PII for personnel administration is 5 USC
Yes	PII about individuals for Bank Secrecy Act compliance 31 USC
Yes	Information by CI for certain money laundering cases may be 18 USC

6f. Has the authority been verified with the system owner? Yes

B.1 BUSINESS NEEDS AND ACCURACY

7. 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.

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) CI .WAV Files - Collected voicemail messages will be received by all CI personnel to support investigative actions. 4) Information collected during softphone calls are discussed in support of the IRS mission. For all intents and purposes the softphone is a transport mechanism and not an actual storage container. For example, PII may be discussed internally via a softphone call, displayed during a softphone video session, transmitted in an instant message, or transferred in a file. PII may be discussed externally via a softphone phone call (video, chat, and file sharing services are not available with external users). 5) IRS user SEID and other data is stored in the Call Manager application and regularly synchronizes with the data stored in the Microsoft Active Directory environment. This information is currently available via the current Microsoft Office suite of tools including Outlook and the Office Communications System (OCS). 6) Information collected during a CWMS session is discussed and presented in support of the IRS mission. For all intents and purposes the CWMS application is a transport mechanism and not an actual storage container. For example, PII may be discussed via a teleconference or discussed and/or displayed during an interactive web conference. Internal [IRS] participants are authenticated and authorized via the IRS single sign-on application. External participants can access meetings by dialing in to the teleconference from an external number or accessing the meeting via a web link provided through a Microsoft Outlook Calendar invite. Detail Records are generated for CWMS teleconferences and web conferences. The following information is contained in these records which are only accessible by system administrators approved via the OL5081 application: - Participant Phone Number - Participant name (as entered by the participant attending on-line web conferences via the web). For external callers, this is not available. - System-related SBU information, such as IP addresses, used to monitor CWMS performance during teleconferences and web conferences. CWMS is primarily a transport mechanism. As a result, no PII is stored, processed, or maintained by the CWMS application that is accessible to other personnel. Hosts may Record CWMS sessions in support of the IRS Mission. The potential exists for PII to be discussed and displayed during a recorded session. This information is centrally-stored in the CWMS database and is only accessible to the Host.

8. How is the SBU/PII verified for accuracy, timeliness, and completeness? Explain how steps are taken to ensure that all information maintained by the system that is used by IRS to make any adverse determination about an individual's rights, benefits, and/or privileges is maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination

There are no mechanisms in place for adjudicating the accuracy, timeliness or completeness of PII. PII may be shared inadvertently during a CWMS session via discussion and/or application sharing. CWMS sessions may be recorded by the Host. The CWMS only records the audio, video and screen captures from the CWMS. The software cannot make any changes to the files once recorded

C. PRIVACY ACT AND SYSTEM OF RECORDS

9. Are 10 or more records containing SBU/PII maintained, stored, and/or transmitted by or through this system? Yes

9a. If **yes**, are records in the system retrieved by any personal identifier (e.g., name, SSN, Photograph, IP Address) for an individual? Yes

If **yes**, is there a System of Records Notice(s) or SORNs that addresses the PII records in this system? Yes

If **yes**, enter the SORN number(s) and the complete the name of the SORN.

SORNS Number	SORNS Name
Treas/IRS 34.037	IRS audit log and security records system
Treas/IRS 00.001	Correspondence Files and Correspondence Control Fi

If **yes**, does the System of Records Notice(s) (SORN) published in the Federal Register adequately describe the records as required by the Privacy Act? Yes

D. RESPONSIBLE PARTIES

10. Identify the individuals for the following system roles. # # Official Use Only

E. INCOMING PII INTERFACES

11. Does the system receive SBU/PII from other system or agencies? Yes

11a. If **yes**, does the system receive SBU/PII from IRS files and databases? Yes

If **yes**, enter the files and databases.

System Name	Current PIA?	PIA Approval Date	SA & A?	Authorization Date
Cisco Unified Communications Manager (CUCM)	Yes	10/28/2013	Yes	11/21/2012

F. PII SENT TO EXTERNAL ORGANIZATIONS

12. Does this system disseminate SBU/PII? No

G. PRIVACY SENSITIVE TECHNOLOGY

13. Does this system use social media channels? No

14. Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.? No

15. Does the system use cloud computing? No

16. Does this system/application interact with the public? No

H. INDIVIDUAL NOTICE AND CONSENT

17. Was/is notice provided to the individual prior to collection of information? Yes

17a. If **yes**, how is notice provided? Was the individual notified about the authority to collect the information, whether such is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects, if any, if they decide not to provide any of the requested information?
A notice will be provided in meeting invites to address the following: You have been invited to a WebEx meeting which enables collaboration with external partners. Therefore, ensuring you adhere to IRS policies on Sensitive But Unclassified (SBU) and Personally Identifiable Information (PII) information is CRITICAL. The meeting host will state the following "This meeting may be recorded for quality assurance purposes."

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

18a. If **yes**, describe the mechanism by which individuals indicate their consent choice(s):
Individuals can choose to not provide the information by not sharing or by not attending.

19. How does the system or business process ensure due process regarding information access, correction and redress?
Convergence users (IP Desk Phone, softphone, and ViewMail) can access a centrally-hosted web page to view, edit, and personally update their data. Detail Records are generated for CWMS

teleconferences and web conferences. The following information is contained in these records which are only accessible by system administrators approved via the OL5081 application: - Participant Phone Number - Participant name (as entered by the participant attending on-line web conferences via the web). For external callers, this is not available. - System-related SBU information, such as IP addresses, used to monitor CWMS performance during teleconferences and web conferences. No PII is stored, processed, or maintained by the CWMS application that is accessible to other personnel. PII and SBU data may be displayed or discussed during CWMS web conference or discussed during a CWMS teleconference. CWMS session recordings are centrally-stored in the CWMS database, They are only accessible to the authenticated Host that generated them. Taxpayers continue to have the right to redress on all tax issues, pursuant to existing IRC and IRM requirements. This tool has the potential to assist in achieving those results, when used to communicate with taxpayers.

I. INFORMATION PROTECTION

20. 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

21. The following people have access to the system with the specified rights:

IRS Employees? Yes

IRS Employees?	Yes/No	Access Level (Read Only/Read Write/ Administrator)
Users	No	
Managers	No	
Sys. Administrators	Yes	Administrator
Developers	No	

Contractor Employees? Yes

Contractor Employees?	Yes/No	Access Level	Background Invest. Level
Contractor Users	No		
Contractor Managers	No		
Contractor Sys. Admin.	Yes	Administrator	Moderate
Contractor Developers	No		

21a. How is access to SBU/PII determined and by whom? No restrictions are in place for normal Convergence operation. The PII data available for access in these applications is required for their operation. CDRs are generated for TIGTA/CI personnel upon request ONLY by cleared IRS Convergence System Administrators. Detail Records are generated for CWMS teleconferences and web conferences. The following information is contained in these records which are only accessible by system administrators approved via the OL5081 application: - Participant Phone Number - Participant name (as entered by the participant attending on-line web conferences via the web). For external callers, this is not available. - System-related SBU information, such as IP addresses, used to monitor CWMS performance during teleconferences and web conferences. No PII is stored, processed, or maintained by the CWMS application that is accessible to other personnel. CWMS is primarily a transport mechanism. As a result, PII and SBU data may be displayed or discussed during CWMS web conference or discussed during a CWMS teleconference. CWMS Session recordings are

only accessible by the Host. They must authenticate via the IRS PIV card and SSO capability. Only IRS employees or IRS contractors with a PIV card can host a meeting.

21b. If computer matching occurs, can the business owner certify that it meets requirements of IRM 11.3.39 Disclosure of Official Information, Computer Matching & Privacy Protection Act? Not Applicable

I.1 RECORDS RETENTION SCHEDULE

22. 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

22a. 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.

The Convergence system is essentially a non-recordkeeping systems and does 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, 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. All records housed in the CWMS system will be erased or purged from the system in accordance with approved retention periods. CWMS data has National Archives approval to affect records disposition. Any records generated and maintained by the system will be managed according to requirements under IRM 1.15.1 and 1.15.6, and will be destroyed using IRS General Records Schedule (GRS) 3.2, item 030, and as coordinated with the IRS Records and Information Management (RIM) Program and IRS Records Officer. CWMS session recordings are centrally stored in the CWMS database. They are only accessible by the authenticated host that generated the recording(s). CWMS session recordings are stored until file space is exhausted, at which time the recordings are overwritten in oldest - newest sequence. Recorded sessions are approved for destruction under General Records Schedule 21 for Audio Visual Records, Item 17- Meeting Recordings and may be destroyed when 2 yrs. old. (N1-GRS-98-2, item 41)

I.2 SA&A OR ECM-R

23. Has the system been through SA&A (Security Assessment and Authorization) or ECM-R (Enterprise Continuous Monitoring Reauthorization)? Yes

23a. If **yes**, what date was it completed? 10/20/2016

23.1 Describe in detail the system s audit trail. Internal Caller information (IRS employees and Contractors) is stored in the Call Manager application and routinely synchronized with Microsoft Active Directory application. This information includes Name, SEID, Location information (GSA Building Code), Email Address, and Phone Number(s). Call Detail Records (CAR) track the results of every phone call placed or received by the Convergence system. They are automatically collected and retained internally by the Convergence system per the retention requirements requested by TIGTA. This data includes call data necessary for tracking call data, such as originating phone, recipient phone, date and time stamp, duration, and other statistical data needed

to determine the quality of the call. Call History data is retained on the IP Desk Phone and the softphone of each user as previously discussed. This includes calls made, calls missed, and calls received. Data includes phone number and name (if available). Voicemail data is centrally stored and encrypted. It is accessible via the IP Desk Phone, the softphone. and the ViewMail application. Access to the stored message requires user authentication. Voice Messages cannot be transmitted to other individuals. However, .WAV files are available for use by CI and TIGTA personnel to support investigative actions. CWMS session recordings are centrally-stored in the CWMS database. They may only be accessed by the authenticated Host that generated them. CWMS detail records are maintained for each meeting conducted. The following data points are collected for each CWMS teleconference/web conference: - originating phone numbers - individual display names as entered by meeting participants - meeting quality and performance metrics - key events / actions, such as enable application sharing, entering / leaving the session, enabling recording, assigning host / presenter privileges, etc. The following information is not collected in the audit log: - voice recordings of participants in teleconferences and web conferences - information displayed and shared online during web conferences

J. PRIVACY TESTING

24. Does the system require a System Test Plan? Yes

24b. If **yes**, Is the test plan in process or completed: Completed

24.3 If **completed/ or in process,** 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? Details for the System Test Plan can be found on the Convergence SharePoint Portal - CWMS Deployment.

24b.1. If **completed**, where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)? The test results are stored on the Convergence SharePoint Portal - CWMS Deployment. A Cybersecurity Penetration Test was previously conducted in August 2015.

24b.2. If **completed**, were all the Privacy Requirements successfully tested? Yes

24.2 If **completed**, are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved? No

K. SBU Data Use

25. Does this system use, or plan to use SBU Data in Testing? No

L. NUMBER AND CATEGORY OF PII RECORDS

26. Identify the number of individual records in the system for each category:

26a. IRS Employees:	Under 50,000
26b. Contractors:	Under 5,000
26c. Members of the Public:	Under 100,000
26d. Other:	No

M. CIVIL LIBERTIES

27. Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment? No

N. ACCOUNTING OF DISCLOSURES

30. 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

End of Report