Date of Approval: **October 25, 2019**

PIA ID Number: **4430**

SYSTEM DESCRIPTION

Enter the full name and acronym for the system, project, application and/or database.

Convergence Cisco Webex Meeting Server, CWMS

Is this a new system?

No

Is there a PCLIA for this system?

Yes

What is the full name, acronym and milestone of the most recent PCLIA?

Convergence/Jabber/WebEx UC. 1766

What is the approval date of the most recent PCLIA?

7/26/2017

Changes that occurred to require this update:

Expiring PCLIA

Were there other system changes not listed above?

No

What governance board or Executive Steering Committee (ESC) does this system report to? Full name and acronym.

User and Network Services (UNS) Governance Board

Current ELC (Enterprise Life Cycle) Milestones:

System Development/Milestone 4B

Operations & Maintenance (i.e. system is currently operational)

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

Yes

GENERAL BUSINESS PURPOSE

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 was established to refresh end of life telephone 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.

PII DETAILS

Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any other type of Sensitive but Unclassified (SBU) information or PII such as information about IRS employees or outside stakeholders?

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

What types of tax identification numbers (TIN) apply to this system?

Social Security Number (SSN)

List the approved Treasury uses of the SSN:

When there is no reasonable alternative means for meeting business requirements

Explain why the authorized use(s) above support the new or continued use of SSNs (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.

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

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.

Employer Identification Number

Other Taxpayer Identification Number

Does this system use, collect, receive, display, store, maintain or disseminate other (non-SSN) PII (i.e. names, addresses, etc.)?

Yes

Specify the PII Elements:

Name

Mailing address

Phone Numbers

E-mail Address

Date of Birth

Place of Birth

Standard Employee Identifier (SEID)

Mother's Maiden Name

Internet Protocol Address (IP Address)

Criminal History

Medical Information

Certificate or License Numbers

Vehicle Identifiers

Passport Number

Financial Account Numbers

Photographic Identifiers

Employment Information

Tax Account Information

Centralized Authorization File (CAF)

Does this system use, collect, receive, display, store, maintain, or disseminate SBU information that is not PII?

Yes

Specify the types of SBU from the SBU Types List (SBU List)

Agency Sensitive Information Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission

Procurement sensitive data Contract proposals, bids, etc.

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.

Proprietary data Business information that does not belong to the IRS

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

Physical Security Information Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities

Criminal Investigation Information Information concerning IRS criminal investigations or the agents conducting the investigations.

Are there other types of SBU/PII used in the system?

Yes

Describe the other types of SBU/PII that are applicable to this system.

Federal Tax Information

Cite the authority for collecting SBU/PII (including SSN if relevant

PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, & 6012e(a)

SSN for tax returns and return information is Internal Revenue Code Section 6109

SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397

PII for personnel administration is 5 USC

PII about individuals for Bank Secrecy Act compliance 31 USC

Information by CI for certain money laundering cases may be 18 USC

Has the authority been verified with the system owner?

Yes

BUSINESS NEEDS AND ACCURACY

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.

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.

How is the SBU/PII verified for accuracy, timeliness and completion?

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

PRIVACY ACT AND SYSTEM OF RECORDS

The Privacy Act requires Federal agencies that maintain a system of records to publish systems of records notices (SORNs) in the Federal Register for records from which information is retrieved by any personal identifier for an individual who is a US citizen or an alien lawfully admitted for permanent residence. The Privacy Act also provides for criminal penalties for intentional noncompliance.

Does your application or this PCLIA system pertain to a group of any record from which information is retrieved by any personal identifier for an individual who is a US citizen or an alien lawfully admitted for permanent residence? An identifier may be a symbol, voiceprint, SEID, or other personal identifier that is used to retrieve information.

Yes

Identify the Privacy Act SORN(s) that cover these records.

IRS 34.037 Audit Trail and Security Records

IRS 00.001 Correspondence Files and Correspondence Control Files

RESPONSIBLE PARTIES

Identify the individuals for the following system roles:

Official Use Only

INCOMING PII INTERFACES

Does the system receive SBU/PII from other systems or agencies?

No

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

No

PRIVACY SENSITIVE TECHNOLOGY

Does this system use social media channels?

No

Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.?

No

Does the system use cloud computing?

No

Does this system/application interact with the public?

No

INDIVIDUAL NOTICE AND CONSENT

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

Yes

How is notice provided? Was the individual notified about the authority to collect the information, whether disclosure is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects on the individual, if any, if they decide not to provide all or 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."

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

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.

How does the system or business process ensure 'due process' regarding information access, correction and redress?

Due process is provided for information discussed and presented pursuant to 26 United States Code (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. Convergence users (IP Desk Phone, softphone, and ViewMail) can access a centrally-hosted web page to view, edit, and personally update their data.

INFORMATION PROTECTION

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

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

IRS Employees

System Administrators: Administrator

IRS Contractor Employees

Contractor System Administrators: Administrator

How is access to SBU/PII determined and by whom?

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. No restrictions are in place for normal Convergence operation. The PII data available for access in these applications is required for their operation. Detail Records are generated for CWMS teleconferences and web conferences. Information contained in these records are only accessible by system administrators approved via the Online 5081 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.

RECORDS RETENTION SCHEDULE

Are these records covered under a General Records Schedule (GRS, IRS Document 12829), or has the National Archives and Records Administration (NARA) approved a Records Control Schedule (RCS, IRS Document 12990) for the retention and destruction of official agency records stored in this system?

Yes

How long are the records required to be held under the corresponding GRS or RCS, and how are they disposed of? In your response, please provide the GRS or RCS chapter number, the specific item number, and records series 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 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 5.2, item 020. The Convergence system is essentially a non-recordkeeping systems and does not require National Archives and Records Administration approval for records disposition or retention. GENERAL RECORDS SCHEDULE 5.2: Transitory and Intermediary Records DAA-GRS2017-00030001 DAA-GRS2017-00030002

SA&A OR ASCA

Has the system been through SA&A (Security Assessment and Authorization) or ASCA (Annual Security Control Assessment)?

Yes

What date was it completed?

4/17/2019

Describe 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 (CDR) 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

PRIVACY TESTING

Does the system require a System Test Plan?

Yes

Is the test plan completed?

Yes

Where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)?

Details for the System Test Plan can be found on the Convergence SharePoint Portal - CWMS Deployment.

Were all the Privacy Requirements successfully tested?

Yes

Are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved?

No

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. CWMS is currently in the Operations and Maintenance phase of its lifecycle. Continuous Monitoring (now called Annual Security Control Assessment) occurs annually to ensure that controls remain in place to properly safeguard PII.

SBU DATA USE

Does this system use, or plan to use SBU Data in Testing?

No

NUMBER AND CATEGORY OF PII RECORDS

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

IRS Employees: Under 50,000

Contractors: Under 5,000

Members of the Public: Not Applicable

Other: No

CIVIL LIBERTIES

Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment?

No

Is the system information used to conduct 'data-mining' as defined in the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 804?

No

Will this system have the capability to identify, locate, and monitor individuals or groups of people?

No

Does computer matching occur?

No

ACCOUNTING OF DISCLOSURES

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