EFFECTIVE DATE

(03-08-2023)

PURPOSE

(1) This transmits new IRM 2.28.1, User Network Services (UNS), Unified Communications (UC) policy.

MATERIAL CHANGES

(1) IRM 2.28.1.1 is updated to hold the required Internal Controls. All existing 2.28.1.1 content is updated to 2.28.1.2.

(2) IRM 2.28.1.2.1.1 paragraph 5 has been updated to reflect the change in request system:

- Description changed from OL5081 to BEARS
- Required fields to complete the request form listed

(3) IRM 2.28.1.2.2.2 has been entirely replaced.

- Section title updated from “Cell Phones” to “Satellite Phones”
- Paragraph 1 is replaced with one that relates to Satellite Phones.

(4) IRM 2.28.1.2.2.3 has been modified to include the following:

- Bullet points C-F added to Paragraph 1.
- New Paragraph 2 inserted. All subsequent Paragraphs moved down one. New Paragraph 2 titled “Requirements”. 3 Bullet points added to Paragraph 2.
- Paragraph 4updated to include bullet points E-G.

(5) IRM 2.28.1.2.2.4 has been updated to reflect the following changes:

- Title updated to “Mobile Hotspots”
- Paragraphs 7-10 added

(6) New IRM 2.28.1.2.2.5 has been inserted and titled “Tablets”. All subsequent sub sections in IRM 2.28.1.1.2 have been moved down 1 number.

(7) IRM 2.28.1.2.2.7 Paragraph 1 has been updated to provide more descriptive content.

(8) IRM 2.28.1.2.2.8 has been added.

(9) IRM 2.28.1.2.4 Paragraph 1 has been expanded.

(10) IRM 2.28.1.2.4.9 has been updated to reflect the following:

- Title changed to “Cloud Meeting and Collaboration Services”
- Paragraph 1 updated from CWMS to ZoomGov.
- IRM 2.28.1.2.4.9.1 updates all references from CWMS to ZoomGov

(11) IRM 2.28.1.2.4.9.3 Paragraph 4 removed.

(12) IRM 2.28.1.2.4.9.4 Paragraphs 2-4 removed.

(13) IRM 2.28.1.2.4.10 Removed. All subsequent sections moved up 1 position.

(14) IRM 2.28.1.2.4.11 Title changed to “Issue Direct”

(15) IRM 2.28.1.2.4.12 New section created titled “Zoom for Government (ZoomGov)”

(16) IRM 2.28.1.2.4.13 New section created titled “Microsoft (MS) Teams”

(17) IRM 2.28.1.2.10.2 Paragraph 1 updated to reflect updates to acronyms and related systems.

EFFECT ON OTHER DOCUMENTS

IRM 2.28.1 dated 08-02-2021 is superseded.

AUDIENCE

This IRM is distributed to all personnel associated with operating and maintaining IRS information technology.

Nancy Sieger
Chief Information Officer

2.28.1
Unified Communications (UC) Overview

Table of Contents

2.28.1.1 Program Scope and Objectives
2.28.1.1.1 Background
2.28.1.1.2 Authority
2.28.1.1.3 Responsibilities
2.28.1.1.4 Program Management and Review
2.28.1.1.5 Program Controls
2.28.1.1.6 Terms/Acronyms
2.28.1.1.7 Related Resources
2.28.1.2 Unified Communications
2.28.1.2.1 Voice, Video, and Data Services
2.28.1.2.1.1 Users
2.28.1.2.1.2 Workstation VoIP Equipment and Services
2.28.1.2.1.2.1 IP Desk, Conference, and Soft Phones
2.28.1.2.1.2.2 Headsets
2.28.1.2.1.2.3 User Number Assignments
2.28.1.2.1.2.4 Extension Mobility
2.28.1.2.1.2.5 International Dialing
2.28.1.2.1.2.6 Collect Calls
2.28.1.2.1.2.7 Call Forwarding
2.28.1.2.1.3 FAX Services
2.28.1.2.1.4 Lobby, Reception, and Common Area Phones
2.28.1.2.1.5 Unified Contact Center Express (UCCX)
2.28.1.2.1.6 Personal Use
2.28.1.2.1.7 Acceptable Use
2.28.1.2.2 Mobile Voice, Video, and Data Services
2.28.1.2.2.1 Bring Your Own Device (BYOD)
2.28.1.2.2.1.1 Mobile Voice Activation (MVA)
2.28.1.2.2.2 Satellite Phones
2.28.1.2.2.3 Government Furnished Device (Smartphone)
2.28.1.2.2.4 Mobile Hotspots
2.28.1.2.2.5 Tablets
2.28.1.2.2.6 Virtual Service Delivery (VSD)
2.28.1.2.2.7 Video Relay Services (VRS)
2.28.1.2.2.8 Multimedia Solutions
2.28.1.2.3 Voicemail Messaging Services (VMS)

2.28.1.2.3.1 Unified Messaging - ViewMail
2.28.1.2.3.2 Acceptable Use
2.28.1.2.3.3 3709 Lines
2.28.1.2.3.3.1 Wage and Investment TAC 3709 Lines
2.28.1.2.3.3.2 Taxpayer Advocate Services 3709 Lines
2.28.1.2.4 On-line Meeting and Collaboration Services
2.28.1.2.4.1 Acceptable Use
2.28.1.2.4.2 Security Guidance
2.28.1.2.4.3 Privacy
2.28.1.2.4.4 Awareness
2.28.1.2.4.5 Roles
2.28.1.2.4.6 Best Practices (if applicable)
2.28.1.2.4.7 File Sharing
2.28.1.2.4.8 Compliance and Incidence Reporting
2.28.1.2.4.9 Cloud Meeting and Collaboration Services
2.28.1.2.4.9.1 Roles
2.28.1.2.4.9.2 Features
2.28.1.2.4.9.3 Compliance and Incident Reporting
2.28.1.2.4.9.4 Acceptable Use
2.28.1.2.4.10 SABA Meeting
2.28.1.2.4.10.1 Roles
2.28.1.2.4.10.2 Features
2.28.1.2.4.10.3 Disabled Features
2.28.1.2.4.10.4 System Configuration
2.28.1.2.4.10.5 Compliance and Incidence Reporting
2.28.1.2.4.10.6 Acceptable Use
2.28.1.2.4.10.7 Best Practices
2.28.1.2.4.11 IssueDirect
2.28.1.2.4.11.1 Roles
2.28.1.2.4.11.2 Features
2.28.1.2.4.11.3 System Configuration
2.28.1.2.4.11.4 Best Practices
2.28.1.2.4.12 Zoom for Government (ZoomGov)
2.28.1.2.4.13 Microsoft (MS) Teams
2.28.1.2.5 Emergency Services
2.28.1.2.5.1 Emergency Calling
2.28.1.2.5.2 Emergency Alert Notification System (EANS)
2.28.1.2.5.3 First Response Location Services
2.28.1.2.5.3.1 Users

2.28.1.2.5.3.2 Acceptable Use
2.28.1.2.6 Backup and Contingency Planning
2.28.1.2.6.1 Contingency Planning
2.28.1.2.6.2 Backup of Configurations, Settings, and Records
2.28.1.2.6.3 System/Site Outages
2.28.1.2.6.4 Backup Call Processing Services
2.28.1.2.7 Assistive Technology Equipment
2.28.1.2.8 Site Maintenance
2.28.1.2.9 Site Equipment Lifecycle Maintenance
2.28.1.2.9.1 Replacement
2.28.1.2.9.2 Repurposing
2.28.1.2.9.3 Excessing and Decommissioning
2.28.1.2.10 Incident Management
2.28.1.2.10.1 Tickets
2.28.1.2.10.2 Assignment Groups
2.28.1.2.11 Information Assurance
2.28.1.2.11.1 Roles and Responsibilities
2.28.1.2.11.2 Security Categorization
2.28.1.2.11.3 Control Assessment and Authorization

2.28.1.1
(03-08-2023)
Program Scope and Objectives

(1) **Overview:** To address agency policies regarding services identified as Unified Communications (UC). Unified Communications encompasses voice over IP capabilities, related E911 calling, emergency alerts, voicemail and messaging, and online collaboration. Policy is also provided for site moves and consolidations with respect to local trunks, phones, and other infrastructure. User and Network Services Unified Communications (UNS UC) Voice Services (VS) and UNS UC Technical Services (TS) will accomplish the work outlined in this IRM using the Information Technology Infrastructure Library (ITIL) processes for UC services, with support from other parts of UNS and IRS-IT.

(2) **Purpose:** This IRM section addresses policy regarding the UC infrastructure and its operation and maintenance, and UC services and their use.

(3) **Audience:** All IRS personnel.

(4) **Policy Owner:** Director, Unified Communications

(5) **Program Owner:** Unified Communications (UC), which is under User and Network Services (UNS)

(6) **Primary Stakeholders:** Unified Communications - Technical Services, Video Services, Voices Services, and Advanced Services

(7) **Program Goals:** This IRM provides the fundamental knowledge and policy guidance to connect people, information, and teams to enable comprehensive and effective collaboration while delivering greater user functionality and capabilities for all IRS employees.

2.28.1.1.1
(03-08-2023)
Background

(1) UNS is responsible for the development, implementation and maintenance of this directive. Approval of this directive, including updates, rests with the Associate Chief Information Officer (ACIO) for UNS. All proposed changes to this directive must be submitted to the Information Technology, UNS, Unified Communications organization.

(2) These policies define the Unified Communications policies and apply to all areas of the IRS utilizing these network collaboration functions.

2.28.1.1.2
(03-08-2023)
Authority

(1) All UC activities shall be planned, managed, implemented, and controlled in accordance with all applicable laws, regulations, IRS policies, processes, and procedures. Throughout the lifecycle of hardware and software assets, the following policies apply:

- The Chief Information Officer (CIO) is the official responsible for ownership, management, and control of IT systems. Organizations other than IRS IT are not authorized to purchase, acquire, manage, move, or maintain IT collaboration systems.
- The CIO or the delegated executive shall ensure that necessary budget, labor, tools, and appropriate training are available to implement these IT collaborations systems and processes.
- This process supports the integrity of the data by ensuring compliance with internal and external controls over telecommunications data and hardware.
- Reports shall contain complete, reliable, consistent, and timely information regarding IT collaboration systems.

- The personnel designated or assigned to perform development and management functions on the collaboration systems shall be trained in the standards, processes, and procedures for performing these activities.
- The IRS complies with audit requests from the Treasury Inspector General for Tax Administration's (TIGTA) Office.
- The IRS adheres to Government Accountability Office (GAO) policies and procedures.
- Federal agencies are required to develop software license management policies and procedures. Federal Agencies are also required to prepare inventories of software present on computers to help ensure that softare is used in complains with the law.
- Federal agencies are required to take inventory of their information technology assets and ensure they are not pay for unused software and/or services from 3rd parties.

2.28.1.1.3
(03-08-2023)
Responsibilities

(1) UNS is responsible for the development, implementation, and maintenance of this directive. Approval of this directive, including updates, rests with the Information Technology, UNS, Unified Communications organization. All proposed changes to this directive must be submitted to UNS.

2.28.1.1.4
(03-08-2023)
Program Management and Review

(1) Policies outline a set of plans or courses of action that are intended to influence and determine decisions or actions of a process. Policies provide an element of governance over the process that provides alignment to business vision, mission, and goals.

2.28.1.1.5
(03-08-2023)
Program Controls

(1) The IRS will implement access control measures that will provide protection from unauthorized alteration, loss, unavailability, or disclosure of information. Access control will follow the principle of least privilege and separation of duties. This IRM further defines the access control requirements found in IRM 10.8.1 as they pertain to voice, video, online and other telecommunications and related security requirements.

2.28.1.1.6
(03-08-2023)
Terms/Acronyms

(1) The table below defins acronyms used throughout this IRM section:

Acronym	Definition
ABM	Authorization Boundary Memo
AO	Authorizing Official
ASL	American Sign Language
AT	Adaptive Technology
BOD	Business Operating Division
BYOD	Bring Your Own Device
CDR	Call Detail Record
CIA	Control Implementation Assessments
CI	Criminal Investigation

CUI	Controlled Unclassified Information
DN	Directory Number
E911	Enhanced 911
EANS	Emergency Alert Notification System
EEFAX	Enterprise Electronic Facsimile
EFA	Enterprise Feature Access
EFO	Enterprise Field Office
EM	Extension Mobility
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing System
FMSS	Facilities Management Security Services
FXO	Foreign Exchange Office
GAO	Government Accountability Office
GFD	Government Furnished Device
HCO	Human Capital Office
IDO	IRS Disabilities Office
IM	Incident Management
ISCP	Information System Contingency Plan
ISSO	Information System Security Officer
ITIL	Information Technology Infrastructure Language
ITSM	IT Service management
LEC	Local Exchange Carrier
MVA	Mobile Voice Access
NIST	National Institute of Standards and Technology
NMCC	Network Management Control Center
NTA	National Taxpayer Advocate
OMB	Office of Management and Budget
PCLIA	Privacy & Civil Liberties Impact Assessment
PII	Personally Unidentifiable Information
PIV	Personal Identity Verification
PoA&M	Plan of Action and Milestones

POD	Post of Duty
POTS	Plain Old Telephone Service
RAS	Reasonable Accommodations Services
RMF	Risk Management Framework
SA&A	Security Assessment and Authorization
SAMC	Situational Awareness Management Center
SBU	Sensitive But Unclassified
SCA	Security Test and Evaluation
SAR	Security Assessment Report
SCMR	Security Change Management Requests
SLA	Service Level Agreement
SNR	Single Number Reach
SO	System Owner
SOP	Statement of Procedures
SRA	Security Risk Assessment
SRST	Survivable Remote Site Telephony
SSP	System Security Plan
SWI	Shared Workstation Initiative
TAC	Taxpayer Assistance Center
TAS	Taxpayer Advocate Service
TFO	Task Force Office
TIGTA	Treasury Inspector General for Tax Administration
TNET	Treasury Network
TTY	Text Telephone
UC	Unified Communications
UCAB	Unified Communications Approval Board
UCCX	Unified Contact Center Express
UEM	Unified Endpoint Management
UNS	User & Network Services
VG	Voice Gateway
VMS	Voicemail Messaging Services
VoIP	Voice over IP

VRS	Video Relay Services
VSD	Virtual Service Delivery
VTC	Video Teleconferencing
W&I	Wage and Investment
WR	Work Request
ZoomGov	Zoom for Government

2.28.1.1.7
(03-08-2023)
Related Resources

(1) The following resources support the content found in this IRM section and provide additional information on the processes and procedures related to Unified Communications voice, video, and data services:

- IRM 1.15.2
- IRM 2.13.1.9.4
- IRM 2.149.2
- IRM 2.149.3
- IRM 10.2.8
- IRM 10.2.9
- IRM 10.5
- IRM 10.8.1
- IRM 10.8.26
- IRM 10.8.27
- IRM 10.8.62.3
- IRM 11.3.12
- IRM 21.3.4.3.2

2.28.1.2
(03-08-2023)
Unified Communications

(1) Unified Communications is a part of User & Network Services (UNS)

2.28.1.2.1
(03-08-2023)
Voice, Video, and Data Services

(1) Unified Communications Voice Services combines multiple services such as voice, video and data onto a common network. These combined services on one network:

a. Deliver greater functionality and features
b. Provide a consistent solution across all IRS PODs
c. Decrease cost of transport, maintenance and upgrades

2.28.1.2.1.1
(03-08-2023)
Users

(1) **IRS Personnel.** Defined as individuals (IRS or contractor) that have approved IRS background clearance for IRS network use.

(2) **Criminal Investigation (CI) hosted Task Force Offices (TFOs)** CI has inter-agency agreements with various law enforcement agencies. The IRS will provide voice services for CI hosted TFO's based on the requirements of those agreements.

(3) **Non-IRS Personnel**. Without an approved IRS background clearance, non-IRS personnel will not be provided phone service on the IRS UC Voice over IP (VoIP) phone system, unless an exception has been approved by the UC

approval board or director. Non-IRS personnel may include but are not limited to on-site facilities such as TIGTA, nurse stations, daycare centers, credit union branches, food service providers, and other federal/state agency personnel, as well as IRS contractors who do not have approval for IRS network use such as contractor security guards or mailroom/loading dock contractors. For these non-IRS personnel, alternate solutions will be determined based on the specific site circumstances and required features needed at each site.

2.28.1.2.1.2 (03-08-2023) **Workstation VoIP Equipment and Services**

(1) Included functions and features of IP Desk, Conference and Soft Phones.

2.28.1.2.1.2.1 (03-08-2023) **IP Desk, Conference, and Soft Phones**

(1) Enterprise Standard phone models will be used for IP phone services.

(2) All IP phone models must be IPv6 compliant and have encryption capability.

(3) All IP phone models must be approved for use on the UC VoIP system by the agency's Enterprise Architecture Enterprise Standards Profile, UC approval board (UCAB) and other applicable approval authorities.

(4) 508 Compliant IP phones are provided where needed.

(5) All IP phone models must be ordered via the contract vehicles in place and to the standards documented in the current Statement of Procedures (SOPs).

(6) Softphone use is currently optional. Where a softphone is provisioned, and the user is provisiosned for a Deskphone, the Directory Number (DN) on the user's desk phone will be shared with the softphone. Functionality will be shared between the softphone and desk phone. (voicemail access, calling features, settings, etc..)

(7) Conference phones – The Senior Executive Team and Conference rooms over 120 square feet are eligible for the currently approved VoIP conference phone. Executive offices and Conference rooms under 120 square feet are not eligible for conference phones and will instead use the standard model IP desk phones.

2.28.1.2.1.2.2 (03-08-2023) **Headsets**

(1) Softphone Headset use is voluntary. They are considered a local expense and must be funded using local business funds. Headsets purchased for use with the Softphone must be Cisco compatible.

(2) Headsets for Users in need of Assistive Technology (Section 508). The IRAP office provides adaptive technology (AT), including headsets, to registered IRAP employees.

2.28.1.2.1.2.3 (03-08-2023) **User Number Assignments**

(1) **DID Number Assignment** – Each user will be provisioned one permanent number. The DID number assigned to each person, is dictated by the assigned Post of Duty (POD). In order to maintain the integrity of the numbering scheme for each site, employees will be assigned a number within that site's DID range. Exceptions to this must be approved at UCAB, with concurrence from the Chief, Technical Services. When an individual employee relocates from one POD to another, they will receive a number from the new POD DID number pool. The employee's number from the originating site will be retained for use

at that site. The employees will not be allowed to take their phone number from one POD to another, either on a temporary or permanent basis.

(2) **New DIDs and Employee Number Changes** – There will be circumstances where it is necessary to change an employee's telephone number. This could be due to a requirement to reduce DIDs at a site, relocation to another site, or other scenarios. New number notification will be sent 90 days prior to implementation when circumstances allow. At a minimum, 30 days advanced notice is required. If 30-90 days advance notification to the employee is not available, an option to provide new number notification to callers may be provided after the number change, to equal a total of no more than 90 days. I.e., if only 30 days' notice of a new number is provided, then calls to the old number may be forwarded to a message indicating the number has changed, for up to but no more than, an additional 60 days. Employees are responsible for publishing their new number on voice mail greetings, email signature blocks and correspondence as soon as they are notified of their new number. Once the new number is active, employees are responsible for updating it directly into HR Connect, which will automatically update their new number in Outlook and Discovery Directory. For individual End User moves, a Move ticket must be initiated when relocating to a new Desk or POD to address new number requirements and standards. The ticket process ensures streamlined service as well as regulatory compliance. Changes to employee phone numbers for Business Unit or Site moves are implemented through the UC O&M Site Projects process, in conjunction with FMSS and EFO.

2.28.1.2.1.2.4
(03-08-2023)
Extension Mobility

(1) **Extension Mobility (EM)** is a UC feature that dynamically configures an EM-provisioned phone according to a user's EM profile at login. This feature is available to, and primarily supports, shared workstations under the Shared Workstation Initiative (SWI), workstations assigned to seasonal employees and shift workers at campus locations. Hoteling workstations will not be provisioned for EM. EM may be provisioned to individuals on a limited basis in other circumstances, with appropriate business justification.

2.28.1.2.1.2.5
(03-08-2023)
International Dialing

(1) International dialing, by default, will be turned off system wide.

(2) International dialing may be turned on for specific phones, either temporarily or long-term as the business need dictates, with justification. To be eligible, such phones must be assigned to an individual. To obtain international dialing capabilities, the Business Unit employee or manager must submit a BEARS request.

(3) Authorized users will:

a. Call international numbers for business purposes only
b. Not allow any other personnel to use their phone for international dialing
c. Report to their Business Unit's first level manager immediately if they suspect that their phone may have been used for international dialing by unauthorized personnel

(4) Improper use of international dialing capabilities by a user will result in this feature being turned off for that user.

2.28.1.2.1.2.6
(03-08-2023)
Collect Calls

(1) Collect calls to the IRS will be accepted if the collect call received is in the best interest of the IRS for the sole purpose of conducting business where no other means of voice communication exists.

2.28.1.2.1.2.7
(03-08-2023)
Call Forwarding

(1) Call Forwarding is a feature that will be enabled for all users locally and nationally.

(2) By default, call forwarding to an international number is disabled system wide but may be enabled with appropriate business justification from the Business Unit's first level executive.

(3) Phone calls may only be forwarded to IRS issued or approved telephones. Forwarding to other devices is prohibited.

(4) It is the individual employee's responsibility to ensure they abide by applicable IRMs and other policy regulations.

2.28.1.2.1.3
(03-08-2023)
FAX Services

(1) EEFax. Enterprise Electronic Facsimile (EEFax) is the faxing standard at IRS.

a. IRS Enterprise Electronic Fax (IRS-EEFax) is an electronic fax solution which may be utilized to send and receive fax documents without the need for a fax machine. In most cases, initiating an outbound fax may be achieved by sending an email with an attachment via Outlook. Received faxes are typically routed to an email inbox (individual or group), with the fax content in a PDF attachment.
b. EEFax is available to all employees.
c. Employees not utilizing the IRS-EEFax should contact their manager to determine the correct account based on their individual faxing needs.
d. See the IRS SharePoint site for detailed steps on obtaining IRS-EEFax or reference the condensed Welcome Packages.

(2) Voice Gateway (VG) Appliances

a. Fax machines will be placed on VG appliances as part of an effort to reduce recurring costs associated with analog lines.
b. Any request to move a fax machine to an analog line must be approved through the UC approval process for analog lines.

(3) CI Critical and Secure Faxes

a. Some CI faxes support critical functions as defined by CI such as Fugitive Agents or high volume.
b. In addition, some fax machines may be designated as Secure by CI. CI faxes machines designated as Secure or that support critical functions will always remain on POTS lines, outside of the UC VoIP system. The supporting CI staff will provide a business justification and the purpose of the critical/Secure fax changes.

(4) CI Non-Critical Faxes

a. All non-critical CI fax machines will be connected to VG appliances.
b. At co-located CI sites, CI fax machines will connect to the VG appliance connected to the IRS switch, to support any required legacy fax hardware.
c. At CI-only sites, the VG appliance will be directly connected to the IRS Edge Router, or, optionally, to an IRS switch, if one is located at the site.

Allowing the supporting Enterprise Field Operations group to have visibility and access into the VG appliances.

(5) TIGTA

a. TIGTA fax machines will be connected to TIGTA supplied POTS lines. TIGTA fax machines will not be connected to the IRS IP system via VG appliances nor will IRS supply POTS lines for TIGTA fax machines.

(6) Non-IRS personnel

a. Non-IRS personnel fax machines will not be connected to the IRS network via VG appliances, or other means.
b. Fax machines used by personnel who do not have approved access to the IRS network will be connected to POTS lines. The party responsible for funding the POTS line for a Non-IRS personnel fax will be determined on a case-by-case basis and is subject to the agreement between IRS and the non-IRS personnel.

2.28.1.2.1.4
(03-08-2023)
Lobby, Reception, and Common Area Phones

(1) For lobby, reception or common area phones accessible by the public, the following guidelines apply:

a. In accordance with IRM 10.8.1.4.16.18, VoIP phones shall not be installed or operated in publicly accessible areas that are not controlled by IRS, i.e. public hallways or lobbies that are outside of IRS controlled and supervised space, or within IRS space that is not supervised when accessible to the public.
b. Cyber ISSO has determined that in controlled IRS space such as a TAC walk-in office, a VoIP phone may be installed if required precautions are taken. The phones will be configured to restrict calls to a specified internal number or allow access to specific IRS service numbers. External calls will be blocked. The data port capability will be disabled.
c. In areas where VoIP phones are prohibited, analog phones may be utilized. The analog phones may be connected directly to the LEC, or to an analog Voice Gateway device, based on current UC security policy.

2.28.1.2.1.5
(03-08-2023)
Unified Contact Center Express (UCCX)

(1) Unified Contact Center Express (UCCX) - provides limited Call Center functionality. It is available on the UC VoIP system on a restricted basis, with appropriate business justification and approved UWR.

2.28.1.2.1.6
(03-08-2023)
Personal Use

(1) All IRS personnel are responsible for proper use, care, protection and reporting of telephony property they use or control (see 1.14.4.4. Utilization of Personal Property) such as, but not limited to: IP phones, fax machines, analog phones, headsets, and telephony related assistive technology. Enterprise Field Office personnel are also responsible for the proper use, care, protection and reporting of additional telephony property they control such as, but not limited to: voice gateway routers, paging gateways, VG appliances, and switches.

2.28.1.2.1.7
(03-08-2023)
Acceptable Use

(1) Certain functionalities of the telephony services are subject to acceptable use policies as delineated below. These include, but are not limited to, International Dialing, Voice Mail services, Call Forwarding, Emergency Calls, Personal Use of Government Property, and ANI/Caller ID Unmasking. Users must follow all guidance on appropriate use of Government IT resources; reference IRM Exhibit 10.8.27-1 (06-20-2017), Prohibited Uses of Government IT Resources for additional guidance.

(2) All IRS personnel are responsible for proper use, care, protection and reporting of telephony property they use or control (see 1.14.4.4. Utilization of Personal Property) such as, but not limited to: IP phones, fax machines, analog phones, headsets, and telephony related assistive technology. Enterprise Field Office personnel also are responsible for the proper use, care, protection and reporting of additional telephony property they control such as, but not limited to: voice gateway routers, paging gateways, VG appliances, and switches.

2.28.1.2.2
(03-08-2023)
Mobile Voice, Video, and Data Services

(1) Roles, features, and configuration for mobile devices and satellite phones.

2.28.1.2.2.1
(03-08-2023)
Bring Your Own Device (BYOD)

(1) Bring Your Own Device (BYOD) is the IRS's innovative program that enables employees to use their personal handheld devices to access IRS applications and data that was previously available only with government-issued equipment. Non-bargaining unit and eligible highly to moderately mobile Bargaining Unit employees may apply for the program. Please Note: Access to BYOD is not permitted while traveling outside of the United States, its possessions, and territories. BYOD will have to be removed from your device before travel and then re-installed upon your return to the United States.

(2) Refer to *IRM 10.8.26* for additional information regarding organizational and individual roles and responsibilities related to BYOD.

2.28.1.2.2.1.1
(03-08-2023)
Mobile Voice Activation (MVA)

(1) Bring Your Own Device (BYOD). BYOD allows personnel to bring government authorized cell/smart phones into IRS telephony services using Single Number Reach (SNR) and Enterprise Feature Access (EFA) - Two-Stage Dialing.

(2) Incoming Calls – Single Number Reach (SNR). An incoming call to an IRS IP user configured for SNR will be offered to not only the user's IP desk phone and softphone, but to an authorized cell/smart phone as well. The user can answer the incoming call at either of the phones. Upon answering the call on one of the phones, the BYOD user has the option to hand off or pick up the call on the other phone.

(3) Outbound Calls – Enterprise Feature Access (EFA) Two-Stage Dialing. EFA allows an IRS IP user who is configured for EFA and who is outside the enterprise to make a call as though they are directly connected to the IRS telephony system. This feature is accessed by the user calling a system-configured access phone number (toll free or local access number) from their authorized device. The call is answered and processed by the IRS system. When this system-configured access phone number is called, the system first requires that the incoming phone number matches a configured Remote Destination Profile that can use this feature. If this incoming phone number

matches, the user is prompted to enter a PIN. After PIN validation, the user is prompted to enter the outbound number to dial. There is no provision to make an outbound call through this system unless the incoming phone number matches the Remote Destination Profile.

(4) The EFA and SNR features of BYOD:

a. Allows the user to mask the mobile phone number when sending the caller's caller-ID data on an outbound call from a BYOD device. The IRS masked Caller-ID data is sent as if the user was calling from within the IRS office. The user may elect to use the *82 feature to unmask the Caller-ID data which will supply the called number with the caller-ID data of the user's desk phone number. The Personal cell phone number will never be sent to the called number if the user utilizes the MVA service when placing the call.
b. Enable mobile users to dial internal extensions.
c. Protect the BYOD user's ″personal″ cell phone number.
d. MVA service will only work with the user's approved BYOD phone number. Home phones or other phones are not authorized to use this service. The phone registered for MVA must be in the sole control of the authorized IRS user. It cannot be used for personal use or on phones that other individuals have access to.

(5) Users must request access through the BEARS process. Users must include the following:

a. Employee's Official Name
b. SEID
c. IRS Email Address
d. Registered BYOD phone number to be used for MVA calls
e. POD

(6) MVA and its related features will be configured by the UC Operations Management Group. Enterprise Field Office personnel will not configure or modify MVA or its related features or services.

(7) Terms and Conditions of use. As per the terms and conditions agreed to during the approval process:

a. Users must notify IRS and TIGTA immediately if their BYOD device is lost or stolen or if the phone number of the device is changed.
b. Users must notify IRS immediately if they suspect that their BYOD device has been improperly used by any person other than the authorized user.
c. Users must notify IRS immediately if any criteria used to initially authorize them for BYOD has changed or if they are separating from the Service.
d. If either the associated desk phone or BYOD phone number changes, a corresponding BEARS request must be submitted to have MVA service configured on the new number.

(8) Access Review. Wireless Solutions Services should periodically review the BYOD authorized users to ensure that all authorized users remain with the Service and that their criteria for approved use has not changed.

2.28.1.2.2.2
(03-08-2023)
Satellite Phones

(1) Per Executive Order 12656, Presidential Policy Directive 40, and Federal Continuity Directive 1 and 2; all federal continuity programs must have access to communications with sufficient resilience and contingencies necessary to perform essential functions at primary and alternate locations. Earthquakes, extreme weather events, civil or political unrest, and other situations can cause a failure of the land-based telephone networks (POTS, VOIP, cell, etc.). Satellite phones communicate via satellite in orbit. If the communication networks are overloaded or disabled, satellite phones will still work. Satellite phones ensure connectivity among key government leadership, internal and external elements, essential function partners, and the public under all conditions.

2.28.1.2.2.3
(03-08-2023)
Government Furnished Device (Smartphone)

(1) General Guidelines

a. Requests for a government furnished iPhone will be submitted through the KISAM ticketing system. Any requests received via e-mail or phone will not be accepted.
b. KISAM Requests do not guarantee fulfillment. User will need to provide sufficient justification for the business need. Business Unit BSPs will have to approve the requests, prior to them being fulfilled by the smartphone team. Limited devices are available for distribution.
c. Information Technology (IT) will not provide employees with both a hotspot and an iPhone for the following reasons:
d. The overlap in functionality, given the iPhone can be used as a hotspot
e. The unjustifiable cost associated with one employee having both devices
f. If a Bargaining Unit employee has both a hotspot and an iPhone, they must relinquish one device to comply with the new policy. (Exceptions will be made on a limited case by case basis).

(2) Requirements

a. Mobility Status - Employee must hold a “High” or “Moderate” Mobility designation at the time of request.
b. Equipment Profile - User must be approved for a Smartphone. (Signified by a “1” in the “Smartphone” column) at the time of request.
c. BEARS Entitlement – User must select the PROD USER SMARTPHONE (UEM SERVER) entitlement at the time of the request.

(3) Prioritization

a. No priority will be given on basis of BU\NBU Status, Series, or Grade. Requests will be fulfilled based on approved requests by BSPs.
b. Expedition of formal requests can only be made at the Director level or higher in the requestor’s organization.

(4) Appropriate Use

a. Government furnished devices are to be used for IRS-related work only. The device is restricted to only allow pre-approved applications.
b. Use of personal Apple accounts will be restricted by the Smartphone Administrators.
c. Prior to international travel with your GFD smartphone, please submit a OSGetServices request ticket at least a week in advance to ensure the necessary travel provisions are enabled on your smartphone.

d. Data usage is monitored. If extraordinarily large amounts of data are consumed, IT/UC will contact the user, their manager or the BOD to confirm the legitimacy of use.
e. Non-Usage Policy - If an employee's number (account) shows non-usage for 60 consecutive days, per the vendors' monthly usage report, an email notification will be sent to the employee, with a copy going to the manager of record, asking for a valid reason as to why the device has not been used. At the same time service will be suspended on the line. This will keep the line and number available for the manager to immediately request reinstatement of the employees' service once the manager provides a valid business reason to continue using the phone. If a response is not received from the manager and/or employee within 30-days (60 days non-usage and 30 days of suspension for a total of 90 days) of receipt of the email notification, the service will be canceled on the line and the user will be removed from the Unified Endpoint Management (UEM) server. IRS Furnished Smartphones showing non-usage for 60 consecutive days, service will be suspended. IRS Furnished Smartphones showing non-usage for 90 consecutive days, service will be canceled.
f. Use of the Bluetooth, location services and mobile hotspot feature are approved for use on the smartphone.
g. The use of Directory Assistance (411) on Smartphones is prohibited.

(5) GFD Smartphone Technical Support Issues

a. User must report technical issues by calling Enterprise Service Desk or through KISAM OSGetServices system.
b. Technical issues must be reported in the form of an Incident Management ticket.
c. Technical support reporting will not be accepted through Request Tasks, E-Mail, MS Teams, or informal phone calls.
d. For issues that cannot be resolved by the Enterprise Service Desk, tickets will be escalated to the Mobile Smartphone Team.

(6) Loss or Theft of GFD Smartphone

a. User must report loss or theft of equipment within 24 hours to CSIRC and TIGTA.
b. User must file a report CSIRC, using the online form: *https://www.csirc.web.irs.gov/incident/*
c. A user must also contact TIGTA to report a missing or stolen smartphone at 1.800.366.4484
d. Replacement for lost or stolen smartphone be provided without a CSIRC report number

2.28.1.2.2.4
(03-08-2023)
Mobile Hotspots

(1) General Guidelines

a. Requests for mobile hotspots can only be made through the designated ordering system. Any requests received via e-mail or phone will not be accepted.
b. Requests submitted to the designated ordering system does not guarantee fulfillment. User will need to provide a sufficient justification or business need for the request. Mobile Hotspot Support has the discretion to reject requests.

c. Information Technology (IT) will not provide employees with both a hotspot and an iPhone due to the overlap in functionality, given the iPhone can be used as a hotspot, and the unjustifiable cost associated with one employee having both devices. If a Bargaining Unit employee has both a hotspot and an iPhone, they must relinquish one device to comply with the new policy. (Exceptions will be made on a limited case by case basis.)

(2) Requirements

a. Mobility Status - Employee must hold a “High” or “Moderate” Mobility designation at the time of request.
b. Equipment Profile - User must be approved for a wireless device and ERAP (signified by a “1” in the “Wireless” column, and a “1” in the ERAP column in IT Portfolio) at the time of request.
c. Active VPN Account – User must have an active VPN account at the time of request.

(3) Prioritization

a. No priority will be given on basis of BU\NBU Status, Series, or Grade. Requests will be fulfilled on a first-come, first-serve basis.
b. Expedition of formal requests can only be made at the Director level or higher in the requestor’s organization.

(4) Appropriate Use

a. Mobile Hotspots will not be provided exclusively for telework, as a redundancy for potential network outages, or a combination of the two.
b. Government furnished mobile device will not be provided for the exclusive purpose of becoming telework eligible.
c. Only IRS computers can be connected to the hotspot. Connecting non-IRS computers, non-IRS cell phones, or non-IRS smartphones is not permitted.
d. Mobile hotspots can only be used in the 50 states, Puerto Rico and the US Virgin Islands (USVI).
e. Hotspot devices should only be charged from a wall outlet and should never be plugged into (tethered) the laptop or the docking station of the laptop. Please note: Plugging the device into the laptop/docking station will initiate tethering, which is prohibited by IT Cyber Security and will cause the device to work improperly or not at all.

(5) Mobile Hotspot Technical Support Issues

a. User must report technical issues by calling the Help Desk or through the designated ordering/ticketing system.
b. Technical issues must be reported in the form of an “Incident” or “Problem” Management ticket.
c. Technical support reporting will not be accepted through Request Tasks, E-Mail, MS Teams, or informal phone calls.

(6) Loss or Theft of Mobile Hotspot

a. User must report loss or theft of equipment within 24 hours.
b. User must file a report CSIRC, using the online form: *https://www.csirc.web.irs.gov/incident/*

c. Replacement for lost or stolen hotspot cannot be provided without a CSIRC report number.
d. Replacement must be handled through the Incident Management (IM) ticketing system.

(7) Authorized Regions - IRS furnished mobile hotspot devices can only be used within the United States, Puerto Rico, and US Virgin Islands (USVI) using the device outside of the designated areas is prohibited. International data usage and additional data fees is not permitted.

(8) Non-usage Policy - IRS furnished mobile hotspots showing non-usage for:

a. 90 consecutive days, shall have the service suspended;
b. 120 consecutive days, shall have the service cancelled.

(9) Excessive Usage - IRS furnished mobile hotspots shall not exceed the monthly usage threshold of 22GB.

(10) Loaning or Transferring Hotspots

a. Government-Furnished mobile devices shall only be used by the IRS personnel in which the device was assigned.
b. Employees are not permitted to transfer or loan their hotspot to other employees for any reason. Hotspots are assigned as assets and the assigned recipient is responsible and will be accountable for any and all data usage, damage, and the security of the hotspot.

2.28.1.2.2.5
(03-08-2023)
Tablets

(1) General Guidelines

a. Tablets are non-standard hardware devices and will follow the IRS Work Request (WR) process as per standard Technology Insertion procedures.
b. Requests very limited, devices are available for distribution.

(2) Appropriate Use

a. Government furnished devices are to be used for IRS-related work only. The device is restricted to only allow pre-approved applications.
b. Use of personal tablet accounts will be restricted by the tablet Administrators.
c. Tablet use is prohibited during international travel except when on official government business.
d. Data usage is monitored. If extraordinarily large amounts of data are consumed, IT/UC will contact the user, their manager, or the BOD to confirm the legitimacy of use.
e. Use of the Bluetooth, location services and mobile hotspot feature are approved for use on the tablet.

(3) GFD Tablets Technical Support Issues

a. User must report technical issues by calling Enterprise Service Desk or through KISAM OSGetServices system.
b. Technical issues must be reported in the form of an Incident Management ticket.
c. Technical support requests will not be accepted through Request Tasks, E-Mail, or other communication means.
d. For issues that cannot be resolved by the Enterprise Service Desk, tickets will be escalated to the Tablet Team.

(4) Loss or Theft of GFD Tablets

a. User must report loss or theft of equipment within 24 hours to CSIRC and TIGTA.
b. User must file a report CSIRC, using the online form: *https://www.csirc.web.irs.gov/incident/*
c. A user must also contact TIGTA to report a missing or stolen tablet at 1.800.366.4484
d. Replacement for lost or stolen tablet will not be provided without a CSIRC

2.28.1.2.2.6
(03-08-2023)
Virtual Service Delivery (VSD)

(1) Virtual Service Delivery (VSD) is the use of video communications to allow two or more parties to interact simultaneously. Video communications involves the integration of video and audio signals, giving a similar sense of connection and collaboration as a live meeting. VSD provides virtual face to face service to taxpayers at Taxpayer Assistance Centers (TAC) and partner locations via high definition video technology.

2.28.1.2.2.7
(03-08-2023)
Video Relay Services (VRS)

(1) Video Relay Services (VRS) provides communication tools to the IRS deaf/hard of hearing employees to be used in the performance of their daily work tasks. These communication tools (desktop video phone and/or video enabled soft phone app (Jabber)) are being utilized which provides the ability of the IRS deaf/hard of hearing employee to communicate and participate in IRS work tasks, team meetings, training, and town hall meetings. Using the American Sign Language (ASL), the deaf/hard of hearing employee may use a remote interpreter or make calls directly. This VRS solution has facilitated a modernized work environment and supports an independent work environment within the IRS deaf/hard of hearing community.

2.28.1.2.2.8
(03-08-2023)
Multimedia Solutions

(1) Manages the IRS video conferencing services procures and maintains related audio and video equipment. Facilitates the ability using various video systems, collaboration using multiple communication mediums (Zoom, MS Teams etc.) utilized by various business units across the IRS enterprise. Audiovisual and videoconferencing equipment solutions will be used by the IRS at specified conference rooms within the agency to conduct business as needed. Users must report technical issues by submitting a ticket through the KISAM OSGet-Services system.

2.28.1.2.3
(03-08-2023)
Voicemail Messaging Services (VMS)

(1) UC Technical Services manages the infrastructure and design of the voice messaging and call coverage service for the IRS. The Voicemail Messaging System (VMS) is a nationwide service provided via a centralized and shared infrastructure and employing Cisco Unity Connection voicemail application servers.

2.28.1.2.3.1
(03-08-2023)
Unified Messaging - ViewMail

(1) ViewMail is a computer application that allows users to listen to and manage voicemail in Outlook.

(2) All IRS users are to be provisioned for ViewMail. The use of ViewMail is optional. If a business unit determines that this application should not be used by their employees, the responsibility for restricting usage is solely up to the business unit.

(3) ViewMail is available for individual users. It is not available for general purpose or departmental mailboxes.

(4) Except for CID users, a .wav file of the voicemail will not be provided to the user. Instead, playback of the voicemail will stream securely from the Unity Connection server to the user's desk phone or softphone.

(5) For CID users only, a copy of the voicemail .wav file will be provided to users' email inboxes, via the CID Exchange servers (for archive and journaling). The original copy of the voicemail will remain on the enterprise Unity servers, and the global settings are applicable.

(6) For legal purposes only, an archive of a voicemail .wav file will be made available utilizing the OsGetServices Ticketing system. Law Enforcement Officers, NTEU, and Labor Relation Representatives will need to provide in the request, Voicemail Box Owner's Name, SEID, to and from Phone Numbers, approximate date/time of voicemail, and the name to whom the official archive will be sent.

2.28.1.2.3.2
(03-08-2023)
Acceptable Use

(1) The VMS is not authorized for transmission of classified or sensitive information.

(2) Users' voicemail accounts are to be used to support the IRS mission only.

(3) Voicemails shall only be forwarded to IRS numbers and authorized BYOD numbers. Voicemails shall not be forwarded to unauthorized numbers. Messages shall not be forwarded to non-IRS phone numbers or email accounts.

(4) If a voicemail message is required beyond the standard retention period for legal and investigative reasons, a KISAM ticket must be submitted at least 7 days prior to expiration in order to retrieve and retain the voice message.

(5) Users must follow all other guidance on appropriate use of Government IT resources; reference IRM Exhibit 10.8.27-1 (09-29-2014), Prohibited Uses of Government IT Resources for additional guidance.

2.28.1.2.3.3
(03-08-2023)
3709 Lines

(1) Wage & Investment (W&I) has overall responsibility for implementation and management of section 3709 lines for Taxpayer Assistance Centers (TACs). More information can be found in IRM 21.3.4.3.2.

(2) A dedicated phone number and voicemail box will be provided. The voice services will be provisioned based on TAC 3709 line requirements, as determined by W&I. Currently, callers to the TAC 3709 line will hear an informational recorded greeting, without the option to leave a message.

2.28.1.2.3.3.1
(03-08-2023)
Wage and Investment TAC 3709 Lines

(1) Wage & Investment (W&I) has overall responsibility for implementation and management of section 3709 lines for Taxpayer Assistance Centers (TACs). More information can be found in IRM 21.3.4.3.2.

(2) A dedicated phone number and voicemail box will be provided. The voice services will be provisioned based on TAC 3709 line requirements, as determined by W&I. Currently, callers to the TAC 3709 line will hear an informational recorded greeting, without the option to leave a message.

2.28.1.2.3.3.2
(03-08-2023)
Taxpayer Advocate Services 3709 Lines

(1) Taxpayer Advocate Services (TAS) has overall responsibility for implementation and management of section 3709 lines for TAS sites.

(2) A dedicated phone number and voicemail box will be provided, using a DID from the number range(s) assigned to each site where such a line is required. The voice services will be provisioned based on TAS 3709 line requirements, as determined by TAS.

2.28.1.2.4
(03-08-2023)
On-line Meeting and Collaboration Services

(1) Roles, features, and configuration for On-line meeting and collaboration services are applicable to all IRS-approved On-line meeting and Collaboration Services unless defined in the overview or detailed sections of specific IRS-approved collaboration tools.

2.28.1.2.4.1
(03-08-2023)
Acceptable Use

(1) Internal to IRS

a. IRS personnel may only use IRS-approved online meeting and collaboration services directly supporting the IRS mission and for achieving IRS business requirements.
b. Only IRS personnel (Employees and Contractor staff with approved clearances) may host or lead online meetings and collaboration services offered and approved by the Service.
c. Most of the IRS-approved online meeting and collaboration tools in the IRS environment restrict IRS employee's participation in on-line meetings unless they are using an IRS approved device or connected through IRS network channels.

(2) External to IRS

a. External participants may only attend IRS hosted online meetings and collaboration events that are IRS approved and offer external participation.
b. External participants should only be allowed to attend IRS hosted online meetings and collaboration events by invitation from the meeting creator to prevent unauthorized access.
c. Several of the IRS-approved online meeting and collaboration tools in the IRS environment restrict external non-IRS participation in on-line meetings.

2.28.1.2.4.2
(03-08-2023)
Security Guidance

(1) IRS personnel may not use IRS collaboration tools for non-IRS meetings and should follow the IRM guidance on collaboration tool usage.

(2) Hosts, Presenters, and Participants must always protect against the unauthorized disclosure of PII, SBU, and CUI during the meeting to unauthorized individuals.

(3) Hosts and Presenters are encouraged to read and familiarize themselves with IRM 10.5, Privacy and Information Protection and IRM 10.8.1, Information Technology (IT) Security, Policy and Guidance related to IRS approved online meeting and collaboration.

(4) SBU and CUI may only be displayed or shared with individuals who have a specific "need-to-know" at any time during the meeting. This includes verbal transmission via the audio or video component of the meeting, as well as through information presented via an application share, the Whiteboard tool, the Notes tool, or the Chat capability where applicable. In the event SBU or

CUI is disclosed to unauthorized individuals, it is the responsibility of the Host to immediately report the incident/breach as prescribed above.

(5) Hosts are responsible for assigning privileges and deselecting any private chat capabilities as required.

2.28.1.2.4.3
(03-08-2023)
Privacy

(1) Use only Enterprise Architecture-approved online meeting and collaboration tools if SBU data needs to be conveyed to meeting participants as required and an available feature of the tool.

(2) For approved virtual meeting tools with encrypted communication capability:

a. Ensure that the audience/recipients are authorized to view the material.
b. Share SBU data (including PII and tax information) on a need-to-know basis.

(3) Refer to (PGLD) Privacy Protections IRM guidance for additional information.

2.28.1.2.4.4
(03-08-2023)
Awareness

(1) Some of the IRS-approved online meeting and collaboration tools restrict external calling or dial-in capabilities.

(2) Some of the IRS-approved online meeting and collaboration tools offer video functionality that may allow users equipped with web cameras to initiate and conduct video calls with one another from their IRS-provided laptops / desktops within the IRS network infrastructure.

(3) IRS approved online meeting and collaboration tool usage and availability may be impacted by participant threshold, i.e., once the meeting threshold is met, no additional participants can join the meeting or degradation in service may be experienced. IRS specific network limitations must be adhered to as it applies to coordinating and scheduling meetings.

2.28.1.2.4.5
(03-08-2023)
Roles

(1) Host - Schedules the meeting, opens the meeting, and can perform administrative tasks during the meeting, e.g., muting participant microphones, assigning and transferring Host and Presenter privileges, and ejecting participants.

a. Hosts or Presenters should follow IRS guidance if special access is required for administrative roles in the respective IRS-approved application used.

(2) Presenter - Can share applications or files with on-line meeting participants following guidelines as outlined in the Acceptable Use and Security Guidance, PGLD Online Meeting IRM guidance, and File Sharing sections.

(3) Participant - Participants can view on-line meeting materials as they are presented. Internal and / external participants can join IRS hosted meetings they have been invited to (not all IRS approved Online Meetings and Collaboration tools allow external participation).

a. They may engage in audio or video discussions as deemed appropriate by the host or presenter in accordance with guidelines in place specific to the collaboration tool and guidance as outlined in this document.

(4) Call-in User (if applicable) - Participant can dial in directly using a phone number provided in the meeting invite if the meeting offers that feature.

2.28.1.2.4.6
(03-08-2023)
Best Practices (if applicable)

(1) Organizer:

a. Advise all participants of their responsibilities for protecting PII, SBU, and CUI against unauthorized disclosure.
b. Advise all participants to mute their microphones and only unmute when they are speaking.
c. Share an application or window instead of sharing desktop to avoid background conversations, e-mails, and material visibility to participants.
d. Some IRS-approved online meeting and collaboration tools offer the ability to set meeting options prior to and during meetings to control access and participation.

(2) Recommendations for ERAP participants connecting through IRS VPN:

a. ISP and system conditions for Individuals working remotely can impact the perceived service quality.
b. Rebooting home internet modems and routers prior to the meeting will aide in alleviating internet performance issues.
c. Restarting PCs and reducing open applications will also provide a better overall experience.

2.28.1.2.4.7
(03-08-2023)
File Sharing

(1) Some of the IRS-approved online meeting and collaboration tools offer file sharing functionality.

(2) Best practice recommendation is to only share information and files specific to the audience as required.

(3) Best practice is that presenters / hosts avoid sharing their entire desktop when using IRS-approved online meetings and collaboration tools.

(4) IRS-approved online meeting and collaboration tools may or may not offer presenters or participants the ability to upload or download files associated with meetings. Some tools offer the ability to restrict who can download a copy of a file shared (example: draft or confidential)

(5) Some of the IRS-approved online meeting and collaboration tools provide meeting presenters / hosts the ability to share files or pictures, whiteboards, and PowerPoint Presentation.

2.28.1.2.4.8
(03-08-2023)
Compliance and Incidence Reporting

(1) Any disclosure of PII must be reported within one hour of discovering the incident. A data loss/breach incident involves the loss, theft, breach, or inadvertent unauthorized disclosure of any of the following:

a. PII - Any information that can distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records. Link an individual, such as medical, educational, financial, and employment information.
b. Sensitive but Unclassified (SBU) Information. Any information which if lost, stolen, misused, or accessed or altered without proper authorization, may adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under the Privacy Act.
c. Controlled Unclassified Information (CUI). A categorical designation that refers to unclassified information that does not meet the standards for classified information under Executive Order 12958, but is pertinent to the

national interests of the United States or to the important interests of entities outside the Federal Government, and under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination.

(2) Organizers, Presenters, and Participants must always protect against the unauthorized disclosure of PII, SBU, and CUI during the meeting to unauthorized individuals.

(3) SBU and CUI may only be displayed or shared with individuals who have a specific "need-to-know" at any time during the meeting. This includes verbal transmission via the audio or video component of the meeting, as well as through information presented via an application share, the Whiteboard tool, the Notes tool, or the Chat capability. In the event SBU or CUI is disclosed to unauthorized individuals, it is the responsibility of the Organizer to immediately report the incident/breach as prescribed above.

2.28.1.2.4.9
(03-08-2023)
Cloud Meeting and Collaboration Services

(1) The IRS uses IRS-approved cloud-based (Zoom for Government (ZoomGov) and Microsoft Teams collaboration tools to support on-line, automated meeting and collaboration services. The Microsoft Teams and Zoom for Government (ZoomGov) applications allows approved IRS personnel to host on-line meetings using encrypted voice and video communications over a secured proxy server. The Microsoft Teams and Zoom for Government (ZoomGov) applications enables IRS personnel to meet and collaborate on-line with personnel within IRS, as well as participants outside of the IRS network.

2.28.1.2.4.9.1
(03-08-2023)
Roles

(1) Host – Schedules the meeting, opens the meeting, and can perform administrative tasks during the meeting, e.g., muting participant microphones, assigning and transferring Host and Presenter privileges, and ejecting participants.

a. Host are required to stay up to date on security requirements and procedures laid out by Cybersecurity
b. Hosts are required to ensure anyone presenting on their accounts are aware that they are not to share PII nor sensitive information is shared via a Zoom for Government (ZoomGov) or Microsoft Teams session.
c. Hosts may not share detailed logon information for their account with others.

(2) Presenter – Can share applications or files with on-line meeting participants.

a. Presenters must stay up to date on security requirements and procedures laid out by Cybersecurity.
b. Presenters are responsible to ensure that no PII nor sensitive information is shared via a Zoom for Government (ZoomGov) or Microsoft Teams session.
c. Presenters may not share detailed logon information for their account with others.

(3) Participant – Participants can view on-line meeting materials as they are presented. A participant does not need a host account to join a meeting they have been invited to. They may engage in audio or video discussions.

(4) Call-in User – Participant can dial in directly using a phone number provided in the meeting invite. These participants may not have access to the on-line

meeting. They are identified as “Call-in User #” in the Participant window. All Call-in Users must be identified prior to discussing any sensitive information. Call-in users that are not successfully identified must be ejected by the Host.

2.28.1.2.4.9.2 (03-08-2023) **Features**

(1) The following features have been disabled to reduce the likelihood of unauthorized disclosure of sensitive data.

a. Remote Desktop Control – Individuals cannot transfer control of their desktop to another participant. Likewise, a participant cannot unilaterally take control of another participant’s desktop during a meeting.
b. File Transfer – This feature is globally disabled.
c. Screen Sharing – Participants cannot share their screen. Presenters may display specific application interfaces, such as Microsoft Excel and Word.
d. Recording – Recording capabilities (if available) size limitation and retention policies set by UC.

2.28.1.2.4.9.3 (03-08-2023) **Compliance and Incident Reporting**

(1) Hosts and Presenters are encouraged to read and familiarize themselves with IRM 10.5, Privacy and Information Protection and IRM 10.8.1, Information Technology (IT) Security, Policy and Guidance, prior to participating in a meeting.

(2) Hosts, Presenters, and Participants must always protect against the unauthorized disclosure of PII, SBU, and CUI during the meeting to unauthorized individuals.

(3) SBU and CUI may only be displayed or shared with individuals who have a specific “need-to-know” at any time during the meeting. This includes verbal transmission via the audio or video component of the meeting, as well as through information presented via an application share, the Whiteboard tool, the Notes tool, or the Chat capability as applicable. In the event SBU or CUI is disclosed to unauthorized individuals, it is the responsibility of the Host to immediately report the incident/breach as prescribed above.

2.28.1.2.4.9.4 (03-08-2023) **Acceptable Use**

(1) IRS personnel may only use the IRS-approved collaboration tool Zoom for Government (ZoomGov) and Microsoft Teams and approved features for meetings directly supporting the IRS mission, for achieving IRS business requirements and for US government interagency collaboration efforts such as disaster recovery.

2.28.1.2.4.10 (03-08-2023) **SABA Meeting**

(1) Roles, features, and configuration for SABA meeting.

2.28.1.2.4.10.1 (03-08-2023) **Roles**

(1) Content Manager – uses the Saba Meeting Agenda Builder to create event content to include multiple question input forms known as evaluations. Content Managers are expected to create Agenda Builder files for users who do not have this ability and are included on a public listing located on the VE Resources site for reference by users who need Agenda Builder assistance. This role builds on the Full Event Manager role. Additional permissions to a general user’s account are required to obtain the Content Manager role. The following courses support the Content Manager role:

a. Participant Overview (optional)
b. Presenter Overview (required)
c. Event Leader (required)
d. Event Manager (required)
e. Content Manager (required)

(2) Full Event Manager - Creates, manages, adds enrollment, and pulls reports for any Classroom and/or Webinar type events. Event Managers are expected to create Webinar and/or Classroom events for users without the Event Manager role and are included on a public listing located on the VE Resources site for reference by users who need Event Manager assistance. This role builds on the Event Leader role. Additional permissions to a general user's account are required to obtain the Event Manager role. The following courses support the Event Manager role:

a. Participant Overview (optional)
b. Presenter Overview (required)
c. Event Leader (required)
d. Event Manager (required)

(3) Basic Event Manager – creates, adds enrollment, leads, and manages their own Meeting type events for up to 20 people. These users have no need to create Webinar and/or Classroom type events. No additional permissions are required for this role. This role is part of a general user's ability. The following courses support the Basic Event Manager role:

a. Participant Overview (optional)
b. Presenter Overview (optional)
c. Meeting Events (recommended)

(4) Event Leader - leads and pulls reports for events for which they have been given the Event Leader role. An Event Leader has full control of the event and can override actions performed by a Co-Presenter. An Event Leader is responsible for understanding and using the event tools needed to hold an effective Classroom and/or Webinar event. Due to the number of virtual training events held in Saba Meeting, formal training is recommended for this role. The Event Leader role is obtained when a general user is enrolled as the Event Leader. The following courses support the Event Leader role:

a. Participant Overview (optional)
b. Presenter Overview (required)
c. Event Leader (required)
d. Classroom Events (recommended)

(5) Co-Presenter – presents content and/or helps to facilitate the event. A Co-Presenter can use the leader tools in an event but can be overridden by an Event Leader. Because a Co-Presenter does not have the full responsibility of the event delivery, training is optional. The Co-Presenter role is obtained when a general user is enrolled as a Co-Presenter or when a participant is promoted to Co-Presenter during the event. The following courses support the Co-Presenter role:

a. Participant Overview (optional)
b. Presenter Overview (optional)
c. Event Leader (optional)
d. Classroom Events (optional)

(6) Participant – attends and participates in events. Basic tools available to the Participant include VOIP audio, chat, content viewing, video, interaction tools (yes/no responses, laughter, applause, and raised hand), and polling response. The Participant role is obtained when a general user attends an event via an enrollment instance or via a guest attend link. The following course supports the Participant role:

a. Participant Overview (optional)

2.28.1.2.4.10.2 (03-08-2023) **Features**

(1) Event Types – Three different event types are available: Classroom, Webinar, and Meeting. Depending on the event type used, determines the role needed for scheduling and features available.

a. Classroom Events – created by an Event Manager and best used for small to medium sized events that need more participant interaction and participation. Classroom events are primarily used for virtual training. Maximum enrollment is limited to 2000 per event.
b. Webinar Events – created by an Event Manager and used to deliver content to a large group of people and when participant interaction will be limited or needs to be controlled. These type events should be used for large meetings such as town halls. Maximum enrollment is limited to 2000 per event.
c. Meeting Events - created by anybody with a Saba Meeting registered user account and used for just-in-time ad hoc meeting needs for small groups and when basic participant interaction is expected. Maximum enrollment is limited to 20 per event.

(2) The event type used determines the features available. Refer to the table below for event type specifics.

Feature	Classroom	Webinar	Meeting
Assigned Presenters – Participants can be promoted to a Co-Presenter while in the event.	Yes	No	Yes
On-line Meeting Participation – Participants can see presentation materials as they are displayed and participate in on-line chat during the meeting with one or more meeting Participants.	Yes	Yes	Yes
Audio Conferencing – VOIP audio allows verbal interaction between Participants and Presenters. Microphone ability is controlled by the Presenters,	Mics all enabled, disabled, or passed one at a time	Mic passed one at a time	Mics all enabled, disabled, or passed one at a time

Feature	Classroom	Webinar	Meeting
Interaction Tools – Participants can respond visually to Presenter actions. Interaction tools include yes/no responses, laughter, applause, raised hand, and step out.	Yes	Yes	Yes
Video Conferencing – All on-line Participants can see other Participants whose video cameras are enabled. Camera display is controlled by the camera owner. Currently two video channels can be displayed.	Yes	Yes	Yes
Application Sharing – Presenters can select and share (display) specific applications that are open on their desktop with participants. Multiple applications can be opened by the Presenter. Share ability can be passed to any Participant in the event.	Yes	Yes	Yes
File Sharing – Presenters can open, and share (display) with Participants, any file that is accessible in a directory on their computer or network. Files can be added for download for Participant copy.	Yes	Yes	Yes
Web Site Sharing – Presenters can add URLS for content display of a web site. This displays the web site in the event and allows Participants to individually interact with the web site while remaining in the event.	Yes	Yes	Yes
White Board – Presenters can create a White Board for interactive editing and sharing with Participants.	Yes	No	Yes

Feature	Classroom	Webinar	Meeting
In-meeting Chat – All Participants may perform on-line chat with one or more meeting participants during the meeting. Note: This feature can be disabled or limited to participant to presenter interaction if sensitive information is being presented and/or discussed.	Yes	Yes	Yes
Breakout Rooms – additional virtual rooms can be created off the main event. Each breakout room has a room leader and a number of participants assigned randomly or assigned by a Presenter.	Yes	No	No
Event Content – all event content, including tool use markers can be added via a Subject. A Subject can be used by any event delivering the same content.	Yes	Yes	No
Reporting – Event Leaders or Event Managers can pull event attendance rosters and evaluation response questions.	Yes	Yes	Yes
Recording – the option to record the event is available via event options. Recordings are available via enrollment or via a guest playback link. All recordings are editable and convertible to .wmv via the Recording Studio.	Yes	Yes	Yes

2.28.1.2.4.10.3
(03-08-2023)
Disabled Features

(1) Video Channels – the number of video channels has been limited to two (2) although eight (8) video channels are available.

(2) Primary Video Channel – due to bandwidth usage, users are not allowed to change a video channel to a primary video channel. This feature allows the video channel to take up half of the content display area while the displayed content takes up the other half.

(3) Telephony Gateway – incorporates conference calls as event audio and allows the conference call to be recorded. Only VOIP audio is available.

(4) Outlook Scheduler– users are not able to create a Meeting type event as part of Outlook meeting scheduling.

(5) Webinar Scheduling – users are not able to use the Webinar Scheduling feature which sends out automatic reminders regarding an upcoming event for which a user was enrolled

2.28.1.2.4.10.4
(03-08-2023)
System Configuration

(1) Saba Meeting system configuration is based on a series of application properties and settings. It has a main domain (Internal Revenue Service) which is used by all IRS employees and contractors and a sub domain (VE Training) which is used for Saba Meeting application training classes.

(2) Login page – accessed a virtual URL *https://ve.learning.irs.gov*Note: Saba can now be accessed using MS Edge.

a. Banner bar – displays help links for how to create an event flowchart, troubleshooting, application overview, questions (FAQ), and additional resources. This banner is displayed on all Saba Meeting application pages.
b. Message area – displays notices and reminders to users.
c. New User section – provides a link for the user to create their account, reminder not to create a duplicate account, and account instructions for contractors.
d. Login area – user can log into their Saba Meeting account using a login and password. Contractors are provided a link for instructions on access for contractors. This area also contains an email link to report account issues.
e. Login help – a forget your password link is located under the login area for users to have their current login information emailed to them

(3) My Schedule page – initial page that appears when any user logs into their account.

a. Left-hand navigation – contains all the items available to that user based on their level of permissions within Saba Meeting. This navigation is broken out by sections to include domain user abilities, Event Manager, Content Manager, and Administrator.
b. Enrollment area – four tabs Upcoming, Ongoing, Recordings, and Past group the user's events based on duration and whether the event is recorded. The only events that appear under these tabs are the events for which the user has been enrolled

(4) User Accounts – required fields for a user account are login, password, first name, last name, IRS phone number, their organization at the BU level, and SEID. Optional fields are title and teleconference information. User accounts also include what groups in which they have been placed for their permission level or further identification.

(5) Security settings:

a. Passwords – required to be changed every 120 days and must contain at least 8 alpha/numeric characters with two of those characters being special.
b. Guest attend – guest attend links are available for users to attend an event for which they have not been enrolled specifically.
c. Access – no external customers can access Saba Meeting

(6) Notifications – users receive notification when enrolled in an event, invited to a meeting, or when an enrolled event's day or time has changed.

(7) Client – the browser client is used for event access.

(8) Video:

a. Channels – limited to two.
b. Channel frame size – the primary channel frame is set to 320x240. The secondary channel frames size is set to 160x120
c. Video size – both the full and normal video size are set to 176x144

(9) Audio:

a. Codecs – includes Medium (ILBC) and High (ISAC). Default audio codec is Medium (ILBC).
b. Up two four (4) event attendees can talk concurrently. The default is set to two (2).

(10) Enrollment limit – limits are set when the event is created. Default limit is 20. These limits are set based on the number of potential attendees. If a meeting enrollment limit is met, the user receives a message that says enrollment is full. At that time, additional enrollment allowance can be set by an Event Manager. An additional notice can also be utilized when creating the event. This notice sends an email to a specified person based on the number of current enrollments. This prevents the attendees from getting an enrollment full message. Due to additional IRS network restrictions, no enrollment can be beyond 2000 participants if the event uses live video. To ensure an overall effective event experience, an overall enrollment has been set to 2000 participants per event.

(11) Licensing limit – 10,000 concurrent licenses can be used at any given time. These licenses are split between the Main domain (9700) and the VE Training subdomain (300). As events are created, licenses used are based on the event's set enrollment limit. Licenses can be moved between the main and sub domains on-the-fly if needed.

2.28.1.2.4.10.5 (03-08-2023)
Compliance and Incidence Reporting

(1) Event Leaders, Co-Presenters and Participants are encouraged to read and familiarize themselves with IRM 10.5, Privacy and Information Protection and IRM 10.8.1, Information Technology (IT), Security, Policy and Guidance, Personally Identifiable Information (PII) prior to participating in a CWMS meeting.

(2) Any disclosure of PII must be reported within one hour of discovering the incident. A data loss/breach incident involves the loss, theft, breach, or inadvertent unauthorized disclosure of any of the following:

a. PII. Any information that can distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records. Or link an individual, such as medical, educational, financial, and employment information.
b. Sensitive but Unclassified (SBU) Information. Any information which if lost, stolen, misused, or accessed or altered without proper authorization, may adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under the Privacy Act.
c. Controlled Unclassified Information (CUI). A categorical designation that refers to unclassified information that does not meet the standards for classified information under Executive Order 12958 but is pertinent to the national interests of the United States or to the important interests of

entities outside the Federal Government, and under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination.

(3) Event Leaders, Co-Presenters, and Participants must always protect against the unauthorized disclosure of PII, SBU, and CUI during the meeting to unauthorized individuals.

(4) PII may not be displayed or shared at any time during the meeting. This includes verbal transmission via the audio or video component of the meeting, as well as through information presented via an application share, imported content, the Whiteboard tool, or the Chat capability. In the event PII is disclosed, it is the responsibility of the Event Leader or Co-presenter to immediately report the incident/breach as prescribed above.

a. If the event is recorded, the Event Leader or Co-Presenter must ensure the Participants understand that no PII or sensitive data should be shown or discussed and get acknowledgement/understanding from the Participants prior to continuing with the event.
b. If the recording does contain missed PII or sensitive data, the recording event association must be set to NO. Thee recording must be edited to remove the PII or sensitive data before it can be made available for playback.

(5) SBU and CUI may only be displayed or shared with individuals who have a specific “need-to-know” at any time during the meeting. This includes verbal transmission via the audio or video component of the meeting, as well as through information presented via imported content, application share, the Whiteboard tool, or the Chat capability. In the event SBU or CUI is disclosed to unauthorized individuals, it is the responsibility of the Host to immediately report the incident/breach as prescribed above.

(6) Event Managers and Content Managers should adhere to the security of the Saba Meeting application as described in the Event Manager and Content Manager training courses. Event Managers and Content Managers should not touch, move, remove, or modify any Saba Meeting item (includes folders, content, events, and recordings) that they do not own unless they have expressed permission by the item owner. That permission should be given in a provable format should conflict occur.

2.28.1.2.4.10.6
(03-08-2023)
Acceptable Use

(1) IRS personnel may only use Saba Meeting for meetings and training with customer internal to the IRS.

(2) IRS personnel may not use Saba Meeting for non-IRS meetings. See IRM Exhibit 10.8.27-1 (09-29-2014), Prohibited Uses of Government IT Resources for additional guidance.

(3) Only IRS personnel and approved IRS contractors can access or lead a Saba Meeting event. At no time should an unapproved contractor or visitor to an IRS facility be allowed to take control of a system running a Saba Meeting event. To ensure only IRS personnel (Employees and Contractor staff with approved clearances) remain in control of the Saba Meeting event, the following actions must be performed.

a. All contractors must have an approved BEARS request prior to Saba Meeting access.

b. All presenters must use their own IRS network access to access the Saba Meeting event.
c. Presenters should verify that no unauthorized personnel are in the event. If an attendee is questionable, the presenter should use the Saba Meeting eject feature to remove attendee from the event.
d. If an unsecure event situation persists, notice to end the event administratively should be provided to one of the Saba Meeting administrators.

(4) All participants should exit the event by clicking on the Exit and Record Attendance button. This ensures attendance reports are accurate.

2.28.1.2.4.10.7
(03-08-2023)
Best Practices

(1) Event Manager:

a. Review the *Need an Event?* flowchart to ensure all sub processes are understood and forms have been submitted.
b. Use the *Saba Meeting Create Event Request Form* to ensure all event settings and options meet the customer's need.
c. Verify enrollment needs to include all live attendance and recording playbacks.
d. Use the Saba Meeting Seat Availability report to avoid creating large events at the same time and to ensure there are licenses available for the event's enrollment needs.
e. Create the event as soon as day and time is confirmed.

(2) Event Leader:

a. If the Event Leader has not completed the Event Leader training, take the one (1) hour Presenter Overview course or review the "The Gist" for Saba Meeting Presenters guide.
b. Become familiar with the Saba Meeting Troubleshooting site to avoid event delays.
c. Review the settings of the event to ensure they meet the needs for event management and content delivery.
d. The Event Leader should practice using the needed event tools, so a comfort level is established.
e. If applicable, discuss all jobs that each co-presenter will perform to include the following: Start/pause/stop/publish the recording, manage microphones, participant interaction to include removing yes/no responses and removing raised hands, chat interactions, and perform participant technical troubleshooting.
f. Review content for an PII or sensitive data and make sure it's loaded to the event.
g. Ensure participant instructions have been sent out based on how event enrollment and access will occur to include participant enrollment, participant self-enrollment, and participants will use a guest attend link sent.
h. Utilize the guides and job aids available on the *VE Resources site*

(3) Co-presenters

a. Practice event job that's been assigned.
b. If delivering content, ensure content is correct and has been practiced. If application sharing will be used, make sure only what will be shared is open. When switching from one shared item to another or moving to.
c. Remind participants that no PII or sensitive data should be discussed.

d. If the event is recorded, get acknowledgment/understanding from the participants.
e. Explain to participants how the event will be managed to include microphone usage: enabled microphones for participants to mute or unmute, passing the microphone one at a time, or complete control of the microphones by the presenters. How questions will be handled: chat, verbal or both. If and how polling questions will be used.
f. Explain to the participants all the participant interaction tools and use to include interaction tools, microphones, volume controls: via audio setup or via event task bar, content resizing, and chat: submit to all or to only the presenters.
g. Keep aware of inappropriate discussions and/or attendees that should not be in the event. Pause the recording or use the eject feature as needed.
h. When the event has ended, make sure all attendees have exited the event.
i. Utilize the guides and job aids available on the *VE Resources site*

(4) Participants:

a. Review the *"The Gist" for Saba Meeting Participant guide* to become familiar with participant tool use.
b. If event attendance requires access to the user's Saba Meeting account, test access to the account prior to event date.
c. Ensure you have the correct audio setup and audio equipment needed to attend the event.
d. Access the event a little early to ensure no access issues occur.

2.28.1.2.4.11
(03-08-2023)
IssueDirect

(1) A webcast is a media presentation distributed over the Internet using streaming media technology to distribute a single content source to many simultaneous listeners/viewers. The webcast platform is a contracted managed service with Issue Direct formerly known as OnStream Media Corporation. The webcasts can be hosted from any of the IRS' 103 Video Teleconferencing (VTC) locations throughout the country and can be seen by a participant on any IRS or non-IRS microcomputer or laptop. This platform has been used since February of 2012 by most IRS Business Operating Divisions (BODs). Webcasting, which allows for virtually real-time video and audio, is the preferred IRS communications platform for large meetings (up to 2,000) since it has been the most stable and reliable platform within the IRS network infrastructure and with limited bandwidth availability.

2.28.1.2.4.11.1
(03-08-2023)
Roles

(1) All IRS users organizing broadcasts for the IRS with Issuer Direct representatives and system are U.S. citizens operating from the U.S. or its territories and have a valid, current IRS background investigation in compliance with FIPS 201, Personal Identity Verification (PIV) of Federal Employees and Contractors.

(2) Equipment involved in this interconnection is used by authorized personnel and is housed in physically secure facilities where physical access is restricted to authorized personnel only.

(3) The Issuer Direct Systems are located at the company headquarters in Raleigh, NC. Their respective locations are identified within their individual system names.

2.28.1.2.4.11.2
(03-08-2023)
Features

(1) The IRS connects to Issuer Direct Webcasts IP. Issuer Direct utilizes, inter alia, IP connectivity to the RMX 4000 video bridge housed in Memphis, Tennessee – by which Issuer Direct can manage the video presentation to attendees.

2.28.1.2.4.11.3
(03-08-2023)
System Configuration

(1) The webcast platform is a contracted managed service with Issuer Direct Corporation, located in Fort Lauderdale, Florida. The webcasts can be hosted from any of the IRS' 103 VTC locations throughout the Country and can be seen, as a participant, on any IRS or NON-IRS microcomputer or laptop. This platform has been used by UNS since February of 2012 by virtually every IRS organization.

2.28.1.2.4.11.4
(03-08-2023)
Best Practices

(1) Have a capacity\network analysis completed before the event.

(2) Pre-event requirements meeting.

(3) Have an equipment check and rehearsal before the event.

2.28.1.2.4.12
(03-08-2023)
Zoom for Government (ZoomGov)

(1) Zoom for Government (ZoomGov) is a cloud platform collaboration tool that allows IRS employees to participate in video and audio conferencing, collaboration, chat and webinars across mobile devices, desktops, telephones and room systems (bandwidth limitations) with internal and external partners. ZoomGov operates in a dedicated secure infrastructure designed to meet federal government FedRamp requirements.

(2) ZoomGov is installed Enterprise-wide on government furnished laptops and workstations (GFE) to allow IRS employees to participate in IRS or other ZoomGov meetings/conferences, both internal to IRS and external (Dept. of Interior, Dept. of Justice, etc.), only if the conference is within the ZoomGov cloud. Due to the security policies in place, access to Zoom Commercial (Zoom.us) through the IRS infrastructure is not permitted.

(3) Since Microsoft Teams is now available in the IRS environment, IRS employees (except for those in CI, who will adopt Teams later) can now use the Teams application for their collaboration needs with internal and external participants. After June 19, 2022, host licenses will be reduced and only a limited number of ZoomGov host licenses will be available to support specific use cases (e.g., Commissioner's Complex, Chief Counsel, and Criminal Investigation).

2.28.1.2.4.13
(03-08-2023)
Microsoft (MS) Teams

(1) IRS has rolled out Microsoft Teams, a new, more secure collaboration platform for employees to meet, chat and work together. MS Teams allows everyone to share files, simplify team interaction, improve collaboration, reduce email traffic and provide a better, faster and more efficient way to work together.

(2) Microsoft Teams is a chat, voice, video and file sharing platform that's part of the Office 365 suite of cloud-based tools. Teams provides a wide variety of approved communication tool features available to the IRS employees to be used in the performance of their daily work tasks. The communication tool provides the ability for IRS employee to communicate and participate in meetings and On-line collaboration with internal and external participants.

(3) MS Teams is the standard collaboration and meeting tool for all employees in the office or while teleworking for internal and external meetings.

2.28.1.2.5
(03-08-2023)
Emergency Services

(1) Emergency calling, emergency alert notification system (EANS), and first response location services.

2.28.1.2.5.1
(03-08-2023)
Emergency Calling

(1) In an emergency (fire, health, safety, etc.) at an IRS POD, users should dial 9-1-1 from the nearest and safest phone - whether that is an IP phone, or a personal or IRS issued cell phone.

(2) Users should not use their softphone to make 911 calls if another phone is safely available, whether they are located at an IRS POD or at a remote location at the time of the emergency.

(3) At specific PODs, users may have been provided additional guidance by FMSS or management for emergency or urgent situations. If additional guidance has been provided for their POD, users should read and follow the guidance provided.

2.28.1.2.5.2
(03-08-2023)
Emergency Alert Notification System (EANS)

(1) EANS is an advanced communications system used to provide real time alerts of emergencies that require action including weather, security, active shooter or other disturbances. System deployment includes a Federal Risk and Authorization Management Program (FedRAMP) authorized cloud solution and desktop and mobile client applications. EANS mobile apps are available to agency personnel to install on personal computing devices. All application servers reside in the cloud with the exception for the component server which syncs user attributes from HRConnect to the cloud servers. Operators (Human Capitol Office) use these attributes (e.g. building code, email address) to send alerts to specific buildings or groups of people.

(2) EANS publishes:

a. Desktop/laptop notifications - pop-up message with audio
b. Mobile alerts - government issued and self-elect personal devices
c. Email notifications - government and self-elect personal email accounts
d. Call to home phone

2.28.1.2.5.3
(03-08-2023)
First Response Location Services

(1) Enhanced 911 (E911) calling capability is available at all IRS posts of duty.

(2) The Situational Awareness Management Center (SAMC) is the focal point for incident reporting related to the Service's physical security. SAMC monitors and routes incident reports to appropriate key IRS personnel.

(3) When a 911 call is placed on a UC VoIP phone, an auto-generated email alert is sent to the SAMC.

2.28.1.2.5.3.1
(03-08-2023)
Users

(1) All IRS personnel may be E911 callers as the situation demands. Anyone with physical access to an IRS IP phone can place an E911 call. This is not limited to a user's assigned phone, during normal operations. At some very large sites, during a network or power outage, 911 access may be limited to certain phones due to hardware limitations. During a network outage, the phones will display a message "Some Capabilities Disabled" which indicates the site has failed over to Survivable Remote Site Telephony (SRST).

(2) All UC VoIP phones (i.e., standard user phones, business unit phones, workstation phones, extension mobility phones, and courtesy phones) support E911 calling.

2.28.1.2.5.3.2
(03-08-2023)
Acceptable Use

(1) The E911 service shall be used to report emergencies only. IRM sections 10.2.9 on Physical Security – Occupant Emergency and 10.2.8 on Physical Security – Incident Reporting provide additional background and guidance.

(2) A softphone should not be used to dial 911 when remotely connected to the IRS network (ERAP). This is because the caller's location cannot be accurately determined and reported by the underlying infrastructure when the softphone is remotely connected to the IRS network, and thus could cause responders to be sent to the wrong location.

(3) In the IRS office setting, a user should always employ an IP phone for 911 calls before using a softphone. Softphones should be a used for dialing 911 as last resort. The location resolution of an IP phone is superior to that of the softphone, aiding emergency responders.

2.28.1.2.6
(03-08-2023)
Backup and Contingency Planning

(1) The IRS UC infrastructure has been constructed for redundancy and automatic failover to a backup call manager component in the event a primary call manager component is down.

(2) Despite the high degree of redundancy and resilience in the UC systems, it remains essential that operations staff follow IRS guidance on contingency planning, and back up of records, configurations and settings.

2.28.1.2.6.1
(03-08-2023)
Contingency Planning

(1) The Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, Appendix III mandates that ″Agencies shall establish policies and assign responsibilities to assure that appropriate contingency plans are developed and maintained by end users of information technology applications."

(2) All operational staff must provide input and identify issues related to the site Disaster Recovery Plan and coordinate activities as required during planned tests and actual emergencies, using a general checklist for contingency planning. UNS has sample forms of general checklists used at the IRS available on their web site at: *http://en.web.irs.gov/default.aspx*. These forms include:

a. Recovery Checklist
b. IT Manager's Checklist
c. Sample On-Site Log
d. Sample Off-Site Log

(3) UC operational staff must adhere to guidance in IRM 10.8.62.3 Contingency Planning.

2.28.1.2.6.2
(03-08-2023)
Backup of Configurations, Settings, and Records

(1) Detailed records must be established and maintained by the local operational staff for the site telecommunications equipment as identified in IRM 2.13.1.9.4, Site Equipment.

(2) The UC TS and UC- Centralized Support staff must develop and maintain a current representation of the logical and physical layout and configurations of the major UC enterprise cores and large Cat 1 cluster components. This representation must include all call control, presence, messaging, emergency calling, call detail record, SSO, and directory interface components, all SIP stack components and trunks connected to the UC system.

(3) The local operational staff must maintain records that document all circuits connecting to the local voice gateway router. These circuits include the backup trunks and the TNET connectivity. These records must include the vendor's circuit identification number(s), type of circuit, and the circuit termination location.

(4) The operational staff must maintain records of any voice circuits at the site which do not connect through the voice gateway router. These records include analog lines from the LEC connected to designated telephones for specific functions and secure fax, modem, and alarm lines. Operational staff must annotate records as to whether the lines are used for fax machines, text-telephone (TTY)-device lines, security-approved modems, or other approved devices. Where applicable, the records must show the analog line's physical location, WSI connections, as well as the assigned device. The operational staff is not required to maintain records of any circuits under the operational control of another organizational unit.

(5) All new system, site, and phone installations and activations must include Call Detail Record (CDR) collection capabilities for the associated end points.

(6) Operational staff members must prepare CDR reports on an as-needed basis. These reports will be treated as ″Official Use Only″ and shared only with authorized individuals with a need to know. Note that the″ Official Use Only″ designation must be approved by IRS officials authorized by Delegation Order No. 89, per IRM 11.3.12, Disclosure of Official Information - Classification of Documents. Requests to provide any such information to personnel, other than operational staff monitoring switch performance, must be made in writing and submitted to the Territory Manager or Computing Center Director. The request must show the name and organization of the requestor and the justification for the request. When the SMDR/CDR records are no longer needed, refer to and follow local site procedures to render these documents unrecoverable. Note: Refer to IRM 1.15.2, Types of Records and their Life Cycles for more information on records management at the IRS.

(7) The operational staff must maintain records of phone number assignments and phone location. These records must be updated by the operational staff at a minimum of once per quarter.

(8) The operational staff must ensure any other records and configuration information required to restore the UC systems are captured and readily available.

(9) The operational staff must ensure that all backup copies are stored off-site. Back-up hard copies of system records will be maintained in off-site Disaster-Recovery storage facilities. Retrieval and restoration of backup materials must be performed in accordance with local procedures.

2.28.1.2.6.3
(03-08-2023)
System/Site Outages

(1) In the event of Telephony Services outage where there is no phone service from the IP phones or softphones, a cell phone can be used, if available.

2.28.1.2.6.4
(03-08-2023)
Backup Call Processing Services

(1) Backup call processing services are provided through Survivable Remote Site Telephony (SRST) and analog lines. In the event the Treasury Network (TNET) connection at the IRS POD is lost, emergency calls will go out the configured Foreign Exchange Office (FXO) port and analog lines, leveraging SRST call processing capabilities on the router.

(2) Dedicated Backup/Emergency analog phones (sometimes also referred to as "Shelter in Place" phones) will not be installed, with these exceptions:

a. There may be instances where agreements have been negotiated between FMSS and other entities. Those agreements must be documented and provided for analog line services to be retained. If appropriate and cost effective, alternate solutions to replace the analog line services may be incorporated i.e., VGs, etc.
b. Backup Phones for Taxpayer Advocate Service (TAS) offices - The National Taxpayer Advocate (NTA) is required by statute under IRC § 7803(c) (4) to maintain independent communications, which includes telephone lines. Based on this requirement, a backup analog phone and line will be provided and placed in the same area as the TAS employees at sites that have a TAS presence. The TAS analog phone will have its own phone number. It will not be a shared line with another phone elsewhere in the building used by other business units. This has been agreed to by the Director of Network Operations and National Taxpayer Advocate Business Modernization BSP. These backup phones are for use by TAS in the event of a local IP network outage due to a power outage or voice gateway failure at the site. The backup phones would then be used by TAS to alert their off-site counterparts/management of the situation and provide them an alternate means of communication to taxpayers until the situation is resolved and the IP phones are working again. The national TAS POCs may waive these requirements at their discretion.
c. Any requests for additional exceptions to this policy must be approved. A business justification must be provided in writing by the requesting entity (FMSS; EFO; other business units) and presented to UNS UC Voice Services.

(3) When analog backup /emergency phones are approved, they should be:

a. Installed in compliance with height requirements as defined within the Americans with Disabilities Act (ADA). This information can be found at *www.ADA.gov*
b. Connected directly to the PSTN, rather than an analog gateway (VG device), thus bypassing the IP system entirely.

(4) Unless they are approved as an exception, existing backup analog phones at sites will be removed and the associated analog lines repurposed or disconnected. Enterprise Field Operations will be responsible for removing the analog phone sets and submitting a disconnect order with their analog line provider (LEC, GSA, etc.) to deactivate the analog lines.

(5) Each existing backup analog phone should be periodically re-evaluated by Enterprise Field Operations to make sure that the requirement has not changed.

(6) In the event of a Telephony Services outage where there is no phone service from the IP phones or softphones, a cell phone can be used, if available.

2.28.1.2.7
(03-08-2023)
Assistive Technology Equipment

(1) The IRAP office provides Assistive Technology (AT), including headsets, software, keyboards, mouse devices and amplifiers, to registered AT users. Users in need of AT must be registered with the IRS Disabilities Office (IDO) or the IRAP Office to obtain AT. If they are not registered with IDO or IRAP, they and their direct manager need to initiate the registration process with their terri-

tory's Reasonable Accommodations Services (RAS) representative. SOPs regarding accommodations for AT customers can be obtained by contacting the IRAP Program Office. All equipment must comply with GSA Government-wide Section 508 Standards.

2.28.1.2.8
(03-08-2023)
Site Maintenance

(1) This section relates to Relocating, Establishing a new site, Changes to Site Population at a Post of duty (POD) and Closing a site.

(2) UC works closely to support EFO on Site relocations, establishing new sites, changes to Site populations and Closing sites, using procedures found in the UC O&M Site Guide.

2.28.1.2.9
(03-08-2023)
Site Equipment Lifecycle Maintenance

(1) Replacement, repurposing, excessing and decommissioning hardware.

2.28.1.2.9.1
(03-08-2023)
Replacement

(1) Paging Gateways - Paging Gateways are under warranty through 1 year after installation. If the Paging Gateway breaks after the warranty period, it is the site's responsibility to get a replacement.

(2) Phones / Headsets / Assistive Technology - EFO is responsible for funding the replacement of broken or malfunctioning desk and conference phones. Individual business units are responsible for the funding and replacement of broken or malfunctioning headsets. Broken or malfunctioning Assistive Technology (AT) should be reported to and replaced through the IRAP office.

2.28.1.2.9.2
(03-08-2023)
Repurposing

(1) When a site moves or closes, all effort must be made to reuse or repurpose UC equipment at another site if it is in good working condition.

2.28.1.2.9.3
(03-08-2023)
Excessing and Decommissioning

(1) Retirement and Excessing of all hardware is covered by *IRM 2.149.3 Asset Management Hardware Procedures*.

2.28.1.2.10
(03-08-2023)
Incident Management

(1) The IRS leverages Information Technology Infrastructure Language (ITIL), a best practices framework which describes how IT resources should be organized to deliver business value, processes, functions, and roles for IT Service Management (ITSM).

(2) Incident Management is an ITIL ITSM process area established to address issues affecting the Unified Communications environment and business service delivery. The goal of incident management is to restore 'normal service operations' as quickly as possible and minimize the impact on business services resulting from technical issues, outages, attacks, compromised operations, etc.

(3) Incident management is related to the following ITIL ITSM processes, including:

a. Change Management. Incident resolution may require initiating a change request. Some incidents may be caused by implemented changes.

b. Problem Management. Problems are recurring issues for which a correction has not been satisfactorily identified. Problem management depends on the accurate collection of incident data to carry out diagnostic activities.
c. Service Asset and Configuration Management. The IRS enterprise configuration management system facilitates the identification of relationships among affected service components.
d. Service Level Management. Service Level Agreements (SLA) define the appropriate levels of 'normal service operation' for IRS business services. A service level breach is an incident and a trigger to the service level management process. SLAs may define timescales and escalation procedures for different types of incidents.

(4) The following IRMs address Unified Communications incident management-related requirements:

a. *IRM 10.2.8, Physical Security Program - Incident Reporting*
b. *IRM 2.149.2, Information Technology Asset Management Enterprise Incident Management Standards*
c. *IRM 10.5.4, Privacy and Information Protection, Incident Management Program*
d. *IRM 10.8.1.4.8 - IR-1 Incident Response Policy and Procedures*

(5) Unified Communications incident management services are primarily provided through the IRS User and Network Services (UNS) organizations as follows:

a. Level 1 - Enterprise Service Desk. Focus is on collecting incident-related data, triage and escalation, and where possible initial resolution. The ESD generates tickets using the KISAM application.
b. Level 2 - Enterprise Field Operations (EFO). Provide direct technical support for sites and personnel. Manage ticket resolution and escalation, as appropriate. Perform MACD on CUCM / CUC devices.
c. Level 3 - Network Management Control Center (NMCC). For issues unable to be resolved by Level 1 (ESD) and Level 2 (EFO), NMCC provides Level 3 support with the exception of application specific UC Collaboration tools.
d. UNS UC Centralized (CG) - CG provides direct technical support for sites and personnel across the IRS enterprise involving issues that cannot be resolved by EFO or the ESD, as well as supporting applications specific to the UC collaboration tools (i.e., Jabber, ViewMail, etc.)
e. Level 4 - UNS UC Technical Services. Address technical issues that cannot be resolved at prior levels. Level 4 support works in close coordination with UC CSG personnel as appropriate to resolve incidents.

(6) Unified Communications maintains an ITIL-compliant Incident Management Plan, tailored to the specific needs of Unified Communications systems, addressing:

a. Incident identification
b. Incident logging
c. Incident categorization
d. Incident prioritization
e. Initial diagnosis
f. Escalation thresholds and protocols
g. Incident resolution
h. Incident closure

i. Communications

2.28.1.2.10.1
(03-08-2023)
Tickets

(1) All issues/incidents involving Unified Communications systems and technologies must be documented and managed within the IRS KISAM Ticketing system.

(2) End users may report issues via the Self-Service application which will initiate incident management processes.

(3) The IRS Enterprise Service Desk will generate Incident Management tickets in accordance with established practices as result of telephone contact with end users.

(4) In addition to the mandatory data inputs for KISAM entries, the following Unified Communications-specific information must be gathered and entered into the IRS KISAM Ticketing system:

a. ASSIGNMENT GROUP
b. SERVICE
c. PROJECT CODE
d. PROGRAM CODE

2.28.1.2.10.2
(03-08-2023)
Assignment Groups

(1) The following assignment groups will support incident handling, status tracking, escalation, and resolution of tickets as appropriate:

a. UNIFIED COMM TECHNICAL OVERSITE CONVERGED VOICE
b. COLLABORATION SVCS – WEBEX
c. VIDEO INFRASTRUCTURE SERVICES
d. ENTERPRISE COLLABORATION SERVICES - EEFAX
e. ENTERPRISE COLLABORATION SERVICES – ENTERPRISE FAX STORAGE
f. ENTERPRISE COLLABORATION SERVICES - Cloud meeting and collaboration services
g. ENTERPRISE COLLLABORATION SERVICES - VSD
h. VIDEO DEPLOYMENT SERVICES
i. VIDEO DEPLOYMENT SERVICES - SABA
j. VIDEO DEPLOYMENT SERVICES VIDEO CONFERENCE SYSTEMS
k. VIDEO DEPLOYMENT SERVICES VIDEO RELAY SYSTEMS

2.28.1.2.11
(03-08-2023)
Information Assurance

(1) Unified Communications is a component of the IRS Information Technology (IT) General Support System 29 (GSS-29), Unified Communications.

2.28.1.2.11.1
(03-08-2023)
Roles and Responsibilities

(1) The following roles and responsibilities are formally assigned and documented in IT GSS-29 security documentation. These roles are responsible for ensuring compliance of the Unified Communications with overarching security requirements as promulgated by law, Federal standards, policy, and guidelines:

a. Authorizing Official (AO) – Authorizes the Unified Communications component for sustaining operations under IT GSS-29. Specifically, the AO is responsible for reviewing the security state of the Unified Communications environment, reviewing identified risks, resolving or accepting risk as appropriate, and coordinating the resolution of identified issues.

b. System Owner (SO) – Oversees the operation and performance of the Unified Communications component and assigns staff to support management, operational, and technical security requirements.
c. Information System Security Officer (ISSO – Ensures security controls are effectively implemented and maintained for the Unified Communications component and is responsible for supporting the development of security-related documentations, to include all Security Assessment and Authorization (SA&A) artifacts, control implementation assessments (CIA), risk-based decision memoranda, etc.

2.28.1.2.11.2
(03-08-2023)
Security Categorization

(1) Unified Communications Federal Information Processing System (FIPS) Publication 199 categorization is:

a. Confidentiality – Moderate
b. Integrity – Moderate
c. Availability – Low

(2) Components of Unified Communications are categorized as follows:

a. Convergence – Moderate
b. EEFAX – Moderate
c. GFSD – Moderate
d. VCS – Low
e. VRS/VSD - Low

2.28.1.2.11.3
(03-08-2023)
Control Assessment and Authorization

(1) The following GSS-29-specific documents are developed in accordance with the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF), Department of Treasury requirements, and IRS-unique requirements and guidelines. The security documents are updated and maintained annually for IT GSS-29 GSS, as well as the level of effort required of the Unified Communications SO and ISSO.

(2) Authorization Boundary Memo (ABM) - An Enterprise-wide GSS-29 Document. Requires up to date Inventory data for all devices and software to include servers, routers, and gateways.

(3) System Security Plan (SSP) - Comprised of two elements; an enterprise-wide GSS-29 overview of high-level security controls to include Unified Communications-specific controls. A Unified Communications-specific appendix addresses controls that are unique to the Unified Communications component and its subcomponents.

(4) Categorization Worksheet - No specific Unified Communications-specific requirements, unless the categorization of Unified Communications changes. The current categorization is Moderate.

(5) Security Risk Assessment (SRA) - Develop risk mitigation plans in response to vulnerabilities, threats, and their associated risks. Risk mitigation strategies must document specific corrective actions and will be documented as a Plan of Action and Milestones (POA&M) finding until resolved.

(6) Information System Contingency Plan (ISCP) - Identify backup plans, reporting hierarchy, escalation strategy, recovery and restoration procedures and a host of required actions to be performed when Unified Communications operations are impacted at the enterprise and site level.

(7) Privacy & Civil Liberties Impact Assessment (PCLIA) - Must be updated to reflect any changes in the presentation or processing of personally-identifiable information (PII) protected by the Privacy Act and Federal guidelines.

(8) Security Test and Evaluation (SCA) results and matrix - Support security testing activities to include providing requested artifacts, enabling access to system components, demonstrating control implementation, etc.

(9) Security Assessment Report (SAR) - Support Annual Security Control Assessment activities. One-third of all security controls are reviewed annually, resulting in the SAR. This document is presented for AO signature and authorization.

(10) Plan of Action and Milestones (POA&M) - Correct identified POA&M entries within specified timeframes and provide regular status updates for outstanding POA&M entries.

(11) Security Change Management SOP - Submit for Security Change Management Requests (SCMR) for significant updates or issues impacting the Unified Communications component.