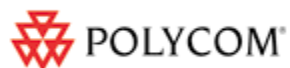


## **The CIO's Guide to Videoconferencing Security: Keeping Pace with the DoD**

March 2010

Study sponsored by:



# Table of Contents

<b>Introduction</b> .....	<b>1</b>
<b>Basic Security Principles – Threats and Best Practices</b> .....	<b>1</b>
Confidentiality.....	2
Integrity.....	2
Availability .....	3
Accountability .....	3
<b>How the Government Addresses VC Security Concerns</b> .....	<b>4</b>
The Security Technical Implementation Guides (STIGs).....	5
Unified Capabilities Requirements .....	6
Product Testing .....	6
Joint Interoperability Test Command (JITC).....	6
STIG Compliance Testing.....	7
Penetration Testing.....	7
Certification and the Approved Product List (APL) .....	8
<b>Solution Spotlight – Polycom RMX 2000 – Multipoint Conference Platform</b> .....	<b>10</b>
Account Management .....	11
Password Management .....	11
Session Management .....	11
Encryption .....	11
Attack Surface Reduction.....	11
Auditing .....	11
Certificates .....	11
Backup and Recovery .....	11
<b>Summary</b> .....	<b>12</b>
<b>About Wainhouse Research</b> .....	<b>13</b>
About the Author(s).....	13
About Polycom .....	14

# Table of Figures

Figure 1: DoD Process for Ensuring Systems Meet Joint Forces Requirements .....	4
Figure 2: DoD Unified Capabilities (UC) Approved Products List (APL) .....	9
Figure 3: Polycom Secure Enterprise Architecture.....	10

## Introduction

Over the past few years, collaboration technologies, like audio, video, and web conferencing, have played an ever-increasing role in national security and defense. This dependency on high impact, rich media communication has spread throughout government and military agencies around the world. Videoconferencing, in particular, has undergone a dramatic transformation from a “nice-to-have” leading-edge technology into a mission critical requirement.

In the military, videoconferencing is now widely used to facilitate real-time decision making for command and control applications and to improve combat effectiveness for wartime fighters. Furthermore, the process of real-time decision-making is transitioning from a “command and control” model to a “command and feedback” model. This paradigm shift gives commanders the ability to know the moment the operational picture changes and improves decision-making in the field.

As videoconferencing has gone mainstream, the concerns of conferencing and communication support teams have shifted. In the past, communication managers focused on basic functionality, reliability, and providing the best possible user experience (as measured in video/audio quality). For the most part, these issues have been resolved thanks to continuous enhancements in hardware, software, and networking technology. Today, the lion’s share of the attention is on the exposure of collaboration tools to IP network security threats. Whether the systems or communication sessions are hosted on secure or non-secure networks, the security threats and concerns are fundamentally the same.

Military organizations such as the U.S. Department of Defense (DoD) and its agencies view security as a holistic wrapper that includes all forms of data transport and the various applications that run on those transport mediums. They have adopted a wide range of policies, procedures, guidelines, security tests, and mandates related to maintaining security for IP communications. This document focuses on the currently accepted DoD security requirements for IP-based videoconferencing.

Although this document specifically highlights security guidelines for the DoD, it is intended to provide insight and information, and act as a model for any organization seeking to deploy a secure visual collaboration environment that meets the DoD strict security requirements.

## Basic Security Principles – Threats and Best Practices

In any secure communications environment, devices and infrastructure items, must meet certain fundamental security requirements before higher-level applications like videoconferencing can be deployed. In today’s information-centric world, the most fundamental security principles of confidentiality, integrity, availability, and accountability have become more important than ever. To meet these requirements, vendors must include numerous security controls and capabilities within their products and services.

## Confidentiality

A communication device must actively preserve the confidentiality of all sensitive information that it stores, processes, transmits, receives, and presents. This means limiting information access to only those authorized to view such information. Items that must be protected include network configuration settings, administrative settings, security settings, user credentials, and of course all data, voice, and video traffic.

Secure environments must consider not only the devices within the environment, but the users as well. This means that administrators must take pro-active steps to protect data from both intentional and inadvertent security leaks. Fundamental requirements include:

- Tight control over the issuing of user accounts
- Prompt removal / disabling of unused or stale accounts.
- Enforcement of strict password guidelines (password length, content, expiration)
- Use of additional identification techniques (e.g. biometrics, digital authenticators)
- Environment-wide policy of granting user privileges on a “must have” basis
- Blocking of inappropriate or unauthorized communications or applications

In addition, information that is transferred between devices and systems must be properly protected using appropriate forms of encryption and cryptography. This includes not only the information payload (meaning the data being sent such as the audio / video traffic itself), but also the signaling information in use as a part of the data transport / transfer, and all control / device management information. At a minimum, secure information must be encrypted with a FIPS 140-2 validated cryptography algorithm. Other encryption technologies, such as the 128-bit Advanced Encryption Standard (AES) commonly used in videoconferencing environments, can then be layered on top of the FIPS protection.

## Integrity

Data integrity refers to the “quality of correctness, completeness, wholeness, soundness and compliance with the intention of the creators of the data.”<sup>1</sup> In a manner similar to the chain of custody used in the legal realm, this means that the information has not been accidentally or deliberately altered in a way that impacts the value or meaning of the data.

A common way to achieve and maintain data integrity is to use digital certificates. Essentially, digital certificates are validation documents, often provided by a 3<sup>rd</sup> party, that verify and establish the identity of one or more participants in a data transaction. The use of digital certificates provides a means of ensuring that the information is being provided by the proper person, device, or system.

In addition to digital certificates, many organizations use digital signatures to verify the identity of the person creating, signing, or sending a document. The proper use of digital signatures gives data recipients a degree of confidence that the information they received was provided by the proper source (a.k.a. authentication) and has not been inappropriately altered (a.k.a. integrity).

---

<sup>1</sup> [http://www.pcmag.com/encyclopedia\\_term/0,2542,t=data+integrity&i=40792,00.asp](http://www.pcmag.com/encyclopedia_term/0,2542,t=data+integrity&i=40792,00.asp)

Devices and systems in use within secure environments should maintain data integrity to the highest degree possible.

## Availability

The proliferation and expansion of IP data networks has paved the way for a number of intentional and unintentional threats to availability. In secure, mission critical environments, systems and networks must be designed to protect the availability of key services and applications. Availability threats can be categorized into several categories including:

- Deliberate threats including hacking, spoofing, and denial-of-service attacks
- Inadvertent threats including configuration changes / environmental modifications
- Device failures and malfunctions
- Issues caused by / related to third party services and systems

To maximize availability in both secure and non-secure environments, organizations should:

- Deploy high performance firewalls with strict access control lists / rule sets
- Limit the number of people able to modify / update system settings
- Define and follow strict backup procedures – including environmental settings
- Implement redundant, distributed, and self-healing architectures
- Deploy products that include ...
  - inherent intrusion detection and auditing capabilities
  - the ability to disable unnecessary functions, and services
- Minimize 3<sup>rd</sup> party / external dependencies to the degree possible

Maximizing availability means balancing cost, convenience, and risk.

## Accountability

An important part of maximizing security is instilling an element of accountability within the environment. This requires proactive tracking and logging of communication sessions and managerial tasks. Key items that should be tracked include:

- User activities (logins, application usage, file transfers, etc.)
- Communication session information (call detail records, etc.)
- Security violations (unauthorized access, repetitive access failures, etc.)

Ideally, the tracking function should provide a) real-time information to allow security personnel to address certain concerns immediately, and b) archived and searchable information enable the identification and resolution of longstanding or complex issues.

The concepts outlined above are intended to provide an overview of basic security concepts and not an all-encompassing view of all potential security risks and recommended preventative measures. However, readers should note that devices intended for use on secure Government networks must address a wide range of security guidelines and recommendations.

## How the Government Addresses VC Security Concerns

Maintaining secure communications systems, networks, and computers is a formidable challenge for any organization. When the information traversing these networks is highly sensitive or relates to the national defense, the stakes become even higher. In 2008, the U.S. Department of Defense “suffered an estimated 80,000 network attacks. On government networks alone, a new software vulnerability is exploited every 82 minutes.”<sup>2</sup>

From the DoD’s perspective, videoconferencing systems are susceptible to a wide variety of security issues. The unauthorized viewing of videoconference sessions is the first type of intrusion that comes to mind. However, many other possible security risks exist including audio-only or content-only snooping, session recording / re-transmission / streaming, unauthorized connections that provide audio / video access to secure areas, and access to information stored on VC systems (e.g. directory information, IP addresses, call logs, etc.).

To help combat this broad set of security challenges, the DoD has established a process for ensuring that systems meet the interoperability and security requirements of the joint forces to ensure information exchange and battlefield success. Simplified, this process includes establishing requirements, performing system testing, and certifying systems once capabilities are verified.



**Figure 1: DoD Process for Ensuring Systems Meet Joint Forces Requirements**

As a part of this process, the DoD maintains a comprehensive set of technical guides, requirements documents, and training courses under the direction of the Information Assurance Support Environment (IASE). The DoD also maintains its own cutting-edge digital crime investigation center, the Department of Defense Cyber Crime Center (a.k.a. the DC3). This section highlights several key tools that the Government uses to safeguard secure information.

---

<sup>2</sup> Source: Aerospace & Defense News, Cyber Security Conference;  
<http://www.asdevents.com/event.asp?ID=611>

## The Security Technical Implementation Guides (STIGs)

The STIGs and their associated checklists provide guidance on the design, development, deployment, operation, and maintenance of U.S. Government Information Systems. Each STIG focuses on a specific product, service, technology, application, or element within a solution. In some cases there are several STIGs covering a particular item or topic. Some of the STIGs that are commonly applied to videoconferencing include:

- Application Security and Development STIG
- Database STIG
- Defense Switched Networks (DSN) STIG
- Network STIG
- Unix STIG
- Video Tele-Conference (VTC) STIG
- Voice Over Internet Protocol (VoIP) STIG
- Web Server STIG
- Wireless Server STIG

For videoconferencing users, the most important security guide is the Video Tele-Conference STIG<sup>3</sup>; an unclassified, 122-page document last updated on 1/8/2008 that includes guidelines for:

- Preventing unauthorized access to VC endpoints
- Protecting the confidentiality of information from unauthorized personnel who may dial into (call) a VC endpoint
- Securing point-to-point, multipoint, and ad-hoc communication sessions
- Preventing the disclosure of sensitive or classified information when using the data sharing capabilities of VC endpoints
- Ensuring that streamed content is not compromised
- Protecting against any security breaches which may result from the use of remote management tools, remote control devices, API touch panels, etc.
- Controlling / restricting access to videoconferencing scheduling systems
- Methods and tasks for maintaining network security including LAN service segregation, wireless LAN access, IP-based boundary crossing issues (e.g. firewalls, port security, etc.)

This STIG also contains a detailed “Quick VTC Endpoint Security Checklist” that covers the basic steps needed to secure an IP-based VTC endpoint.

Vendors and service providers seeking to provide DoD / military clients with secure videoconferencing solutions must ensure that their offerings adhere to the applicable elements of the appropriate STIGs.

---

<sup>3</sup> [http://iase.disa.mil/stigs/stig/vtc\\_stig\\_v1r1\\_010807\\_final.pdf](http://iase.disa.mil/stigs/stig/vtc_stig_v1r1_010807_final.pdf)

## Unified Capabilities Requirements

From a security point of view, videoconferencing is viewed not only as a stand-alone, isolated application, but also as a part of a unified communications (UC) environment. As such, it is subject to the terms, conditions, requirements, and recommendations specified within the Unified Capabilities Requirements (UCRs).

The UCRs expand upon the recommendations provided within the STIGs and specifically focus on products, services, and systems that provide one or more of the following capabilities:

- Voice and Video Conferencing
  - Point-to-Point (2 participants / sites only)
  - Multi-Point (3 or more participants / sites)
- Unified Conferencing / Desktop Conferencing
- Web Conferencing / Collaboration
- Instant Messaging and Chat
- E-Mail / Calendaring
- Unified Messaging
- Mobility

The UCR provides a holistic perspective on Unified Capabilities, from the DoD's perspective, and serves as a reference and guideline for future UC device acquisitions.

Of particular significance in the UCR is the last section that describes the series of testing and validation steps a product must go through to be approved for use in secure environments and added to the appropriate Approved Product List (discussed further below).

## Product Testing

### Joint Interoperability Test Command (JITC)

The Joint Interoperability Test Command (JITC) is a test and evaluation organization responsible for evaluating technology / communications products to be used on secure networks or within secure environments.

JITC provides a full range of standardized and customized tests, evaluation and certification services and works directly with vendors to certify their products. JITC is the only organization authorized to certify Information Technology (IT) and National Security Systems (NSS) for joint and combined use. JITC is also the Operational Test Agency for DISA and other DoD managed programs.

Once a product is scheduled for testing, the product will appear on the DOD Unified Capabilities (UC) Defense Switched Network (DSN) Schedule on the JITC website. Progress can be monitored at <http://jitc.fhu.disa.mil/tssi/schedule.html> (click the link under Schedule).

While JITC testing procedures vary based on the devices under assessment, in general JITC verifies that systems conform to the security requirements and recommendations outlined in ~ 30 documents including but not limited to:

- DoD Instruction (DoDI) 8500.2 - Information Assurance (IA) Implementation
- Federal Information Processing Standards Publications (FIPS Pubs)
- CJCSI 6212.01E - Interoperability and Supportability of Information Technology and National Security Systems
- CJCSI 6510.01D - Information Assurance (IA) and Computer Network Defense (CND)
- Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) Guidance

As a part of the JITC testing, the DoD subjects videoconferencing equipment to a documented battery of attacks and vulnerability tests designed to expose any security vulnerabilities. The goal of this testing is to evaluate the device in question's performance in typical attack situations and conditions that might arise in a real world environment. The testing focuses on two main areas as follows:

#### STIG Compliance Testing

STIG compliance testing verifies that the system under evaluation is configured – or at least configurable – to be in accordance with all applicable STIGs. For example, the Video Tele-Conferencing (VTC) STIG states that, "FECC (far-end-camera-control) should be disabled to prevent the control of the near end camera by the far end unless required to satisfy validated mission requirements." To test for compliance with this STIG recommendation, JITC would verify that the video system allows users / administrators to disable far end camera control.

As a part of the STIG compliance testing, JITC also evaluates the solution's conformance to a number of other items including:

- The applicable IA (Information Assurance) requirements specified in the UCR
- A set of 19 additional IA requirements derived from the GR-815-CORE-2 compliance matrix
- Multiple IA controls from DoD Instruction 8500.2

#### Penetration Testing

Penetration testing aims to circumvent the security capabilities of the system under evaluation in order to compromise the device's ability to maintain the proper level of confidentiality, integrity, and availability.

The testing covers a wide range of potential vulnerabilities such as buffer overflows, integer overflows, format string issues, SQL injection, command injection, and cross-site scripting. In some cases the JITC engineers use internally developed tools and methods. In other cases, industry standard tools such as port scanners, vulnerability scanners, network sniffers, packet analyzers, password crackers, and fuzzers are used. The JITC attack kit includes more than 100 tools, many of which are included in the list of the Top 100 security tools posted on the Insecure.Org website ([www.insecure.org](http://www.insecure.org)).

Two specific test tools worthy of additional coverage are:

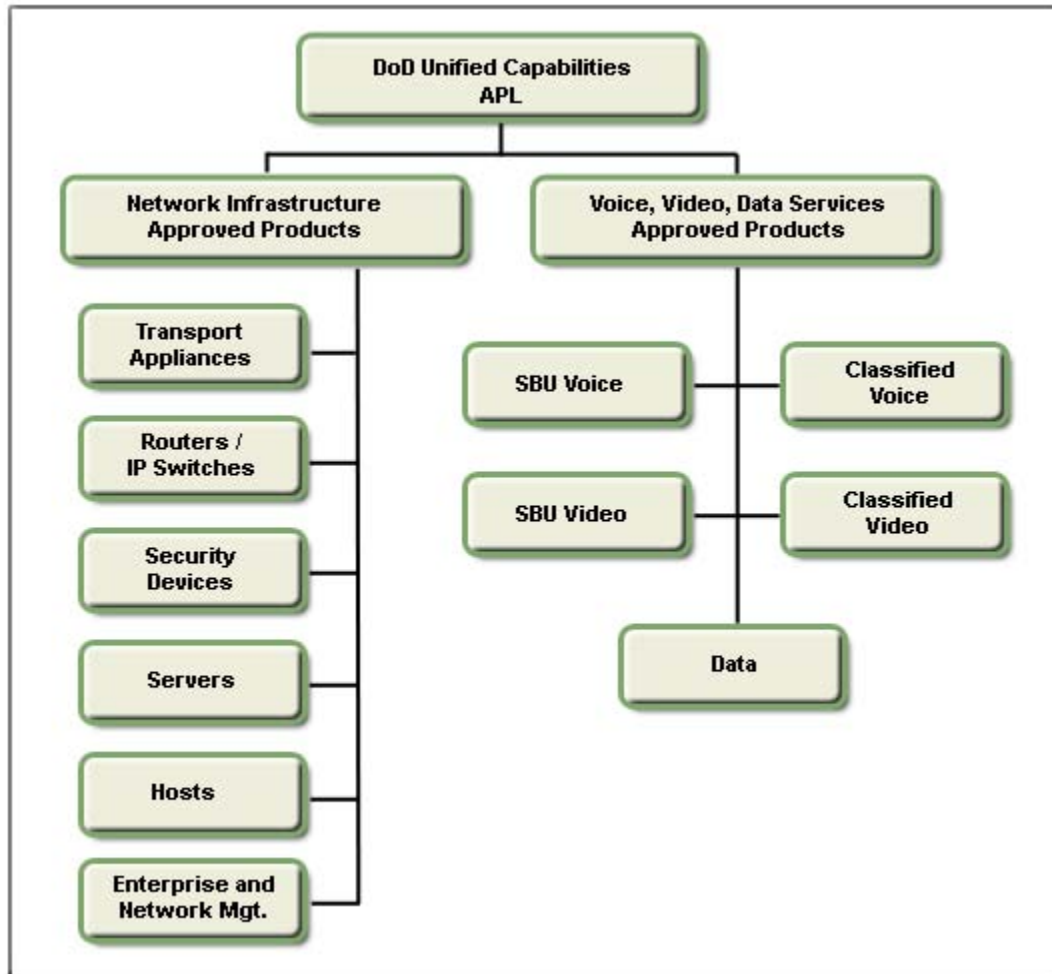
- 1) The DISA FSO Platinum and Gold Disks
- 2) The DISA SRR scripts

These tools allow product developers and JITC test staff to perform a variety of security assessments of operating systems and applications. These tools are especially useful to assess the inherent security of products leveraging embedded operating systems.

### Certification and the Approved Product List (APL)

Upon successful completion of JITC testing, the product is presented to the Defense IA / Security Accreditation Working Group (DSAWG). The DSAWG reviews the test results and assesses the residual risk associated with the use of the product(s) in question in secure environments or on secure networks. If the residual risk is deemed acceptable, the solution receives DoD Defense Switched Network (DSN) Joint Interoperability Certification (JIC) and Information Assurance Accreditation (IA) and is added to a carefully managed list of approved solutions called the Approved Products List (or APL). Only certified products are authorized to be used on Department of Defense (DoD) networks.

Previously there were two APLs that applied to the videoconferencing market; the DoD Unified Capabilities (UC) APL, and the IPv6 APL. However, the DoD no longer requires a stand-alone IPv6 certification. Instead, IPv6 verification is included within the interoperability, information assurance, and functionality requirements covered by the UC APL.



**Figure 2: DoD Unified Capabilities (UC) Approved Products List (APL) <sup>4</sup>**

Accreditation, and the subsequent inclusion on the UC APL<sup>5</sup>, allows vendors to sell their products to DoD agencies and for use over DISA networks. In addition, agencies in need of communication solutions know that products on the APL have passed a specific set of tests and are suitable for use in secure situations.

Note that JITC approval and inclusion on the APL are not perpetual. Approved videoconferencing equipment must be re-assessed every four years.

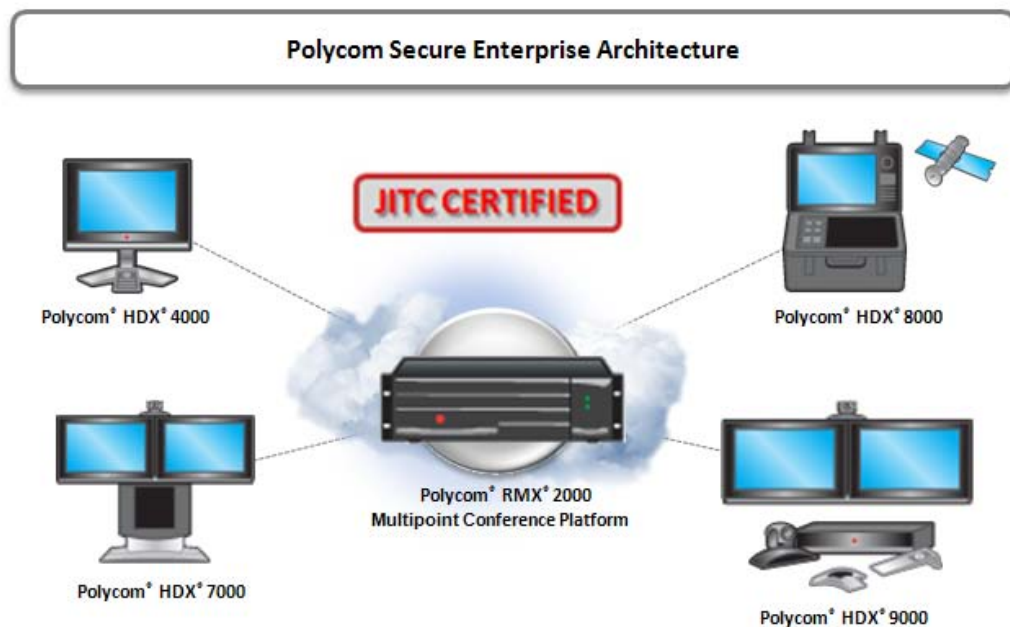
<sup>4</sup> Source: <http://jitc.fhu.disa.mil/apl/index.html>

<sup>5</sup> UC APL: [http://jitc.fhu.disa.mil/apl/dsn/apl\\_vtc.html](http://jitc.fhu.disa.mil/apl/dsn/apl_vtc.html)

## Solution Spotlight – Polycom RMX 2000 – Multipoint Conference Platform

The Polycom RMX is a real-time, standards-based media conferencing platform for the delivery of high quality video, audio, and data collaboration content. The RMX 2000 conferencing platform is designed in accordance with the ATCA (Advanced Telecommunications Computing Architecture) standard and supports large scale, fully redundant, centralized and distributed deployments. Key features of this platform include:

- Support for both centralized and distributed deployments
- Support for H.323, SIP, and H.320 communication protocols
- Support for H.264, H.263, and H.263+, H.263++, and H.261 video protocols
- Support for scheduled and ad-hoc conferencing sessions
- Support for video resolutions ranging from QCIF to HD1080p
- Support for wide-band audio
- Support for H.239 dual streams
- Integrated packet loss protection
- Integrated video upscaling capability to maximize user experience



**Figure 3: Polycom Secure Enterprise Architecture**

The RMX also includes a variety of security features ranging from AES encryption for all media streams to secure conference features that limit the number of attendees and help protect against operator oversight. In order to meet DoD security requirements, the 4.5.0.F version of the RMX software was designed with the following capabilities:

## Account Management

- Use of tiered user accounts
- Ability to disable idle accounts
- Automatic lockout in response to failed login attempts
- Configurable banners (login banner and main RMX web client page)

## Password Management

- Ability to change all default passwords
- Ability to define and enforce password complexity rules
- Disallowing repetitive use of same password
- Forcing password changes based on password age
- Password protection via SHA-1 hash

## Session Management

- Automatic session timeout
- Full tracking of login history (last successful login, up to 10 failed login attempts)
- Full tracking of administrative and operator activities via auditor functionality

## Encryption

- Use of FIPS-140 validated encryption on all management and media streams
- Real-time encryption of media via 128-bit AES
- Storage of sensitive data using SHA-1 hash (one-way encryption)

## Attack Surface Reduction

- Use of hardened and reduced embedded operating system
- Automatic use of Gold Disk to verify security of client PCs
- Use of relatively few management and media ports for daily use
- Presentation of management interfaces on a separate, administration only network

## Auditing

- Full auditing of security related events, login attempts, and critical system changes
- Inclusion of date / time stamps, user IP address and username in all audit records
- Storing of audit logs with read-only permissions (cannot be modified or deleted)
- Logging of all call activity (via call detail record / CDRs)

## Certificates

- Support for installation of DoD-backed certificates for the integrated HTTPS server.

## Backup and Recovery

- Support for offloading of audit logs.
- Ability to backup and restore of system configurations (for fast recovery from outages)
- Ability to revert to hardware-level factory settings

In 2010, the RMX 2000 running version 4.5.0.F completed JITC testing and was added to the Department of Defense Unified Capabilities Approved Products List (UC APL). Other Polycom products on the UC APL include the Polycom HDX video endpoint product family and the Polycom MGC MCU / video bridge.

## Summary

The proliferation of IP networks has increased the need for organizations, and especially government agencies, to take pro-active steps to secure information.

Despite the emergency of countless new products and technologies in recent years, the fundamental principles of data security (confidentiality, integrity, availability, and accountability) still remain. In addition, organizations should recognize that proper data security involves the protection of more than just the obvious pieces of information. For example, in the videoconferencing world, one must protect not only the media streams, but also the information stored within the video endpoints, video bridges, management systems, and other devices within the visual collaboration environment.

In order to address data security concerns, the DoD maintains a comprehensive set of technical guides, requirements documents, and training courses under the direction of the Information Assurance Support Environment (IASE). The DoD also maintains its own cutting-edge digital crime investigation center, the Department of Defense Cyber Crime Center (a.k.a. the DC3). In addition, the DoD has defined and maintained various security assurance documents including the Security Technical Implementation Guides (STIGS) and the Unified Capabilities Requirements (UCRs).

Products to be used in secure environments must pass a strict set of tests conducted by the Joint Interoperability Test Command (JITC) to verify that the systems conform to the applicable security recommendation documents as described above. The JITC test results are then reviewed by Defense IA / Security Accreditation Working Group (DSAWG). Assuming the product passes the DSAWG review, it is added to the DoD UC Approved Products List (APL) and is approved for use on secure networks.

Organizations operating in secure environments should ensure that the products in use not only conform to the appropriate DoD security standards, but also are approved for use on secure networks.

With the release of the 4.5.0.F software release, the Polycom RMX 2000 joins the 20 or so products currently included on the UC APL.

While the majority of this document focused on the needs and concerns of DoD users, enterprise users seeking highly reliable and secure products should leverage the testing performed and policies defined by the DoD. In short, if a product is approved for use in secure military environments, chances are it will meet and exceed the security and reliability requirements of the typical enterprise organization.

## About Wainhouse Research

Wainhouse Research, LLC (WR) provides analysis and consulting on the market trends, technologies/ products, vendors, applications, and services in the collaboration and conferencing fields. Areas of coverage include hardware, software, and services related to audio, video, and web conferencing, unified communications, and enterprise social networking. The Company publishes market intelligence reports, provides customized strategic and tactical consulting and studies, and produces industry events (conferences). Additionally, the Company operates industry-focused and end user-focused Web sites and publishes a weekly sponsored bulletin for news and analysis. For more information on Wainhouse Research, visit [www.wainhouse.com](http://www.wainhouse.com).

### About the Author(s)

Ira M. Weinstein is a Senior Analyst and Partner at Wainhouse Research, and a 20-year veteran of the conferencing, collaboration and audio-visual industries. Prior to joining Wainhouse Research, Ira was the VP of Marketing and Business Development at IVCi, managed a technology consulting company, and ran the global conferencing department for a Fortune 50 investment bank. Ira's current focus includes IP video conferencing, network service providers, global management systems, scheduling and automation platforms, ROI and technology justification programs, and audio-visual integration. Mr. Weinstein holds a B.S. in Engineering from Lehigh University and can be reached at [iweinstein@wainhouse.com](mailto:iweinstein@wainhouse.com).

Andrew W. Davis is a researcher, analyst, and opinion leader in the field of collaboration and conferencing. He is a co-founder of Wainhouse Research. Prior to Wainhouse Research, he held senior marketing positions with several large and small high-technology companies. Andrew has published over 250 trade journal articles and opinion columns on multimedia communications, videoconferencing, and corporate strategies as well as numerous market research reports and is the principal editor of the conferencing industry's leading newsletter, The Wainhouse Research Bulletin. A well-known industry guest speaker, Mr. Davis holds B.S. and M.S. degrees in engineering from Cornell University and a Masters of Business Administration from Harvard University and can be reached at [andrewwd@wainhouse.com](mailto:andrewwd@wainhouse.com).

## About Polycom

(Copy provided by Polycom)

Polycom, Inc. is the global leader in telepresence, video, and voice solutions and a visionary in communications that empower people to connect and collaborate everywhere.

Companies choose Polycom for solutions that allow their workforces to communicate more effectively and productively over distances. Using Polycom unified communications (UC) solutions—telepresence, video, and voice solutions and services—people connect and collaborate with one another from their desktops, meeting rooms, class rooms, and a variety of mobile settings—and from anywhere in the world. In today's economy, our customers wish to cut the time, cost, and carbon emissions associated with gathering the right people in one place to solve problems. Instead of traveling, virtual teams use Polycom solutions to easily and quickly collaborate “face-to-face” wherever they are, which allows them to focus their resources, time, and energy on addressing business challenges.

Collaborating with Polycom solutions has also become a key competitive advantage for leading organizations around the globe. Our customers tell us it makes sense to use Polycom solutions and their existing business applications to communicate and share information in real time over any device and across any network. Polycom's open-standards integration with the leading unified communications (UC) platform vendors makes it possible. Quite simply, it makes good business sense for our customers to rely on the broadest offering of unified communications solutions—from Polycom—so they can improve productivity, reduce their costs, rapidly gain a return on their technology investment—and thrive.