

**BY THE ORDER OF THE COMMANDER
AIR FORCE MATERIEL COMMAND**

AFMC INSTRUCTION 33-105

15 JULY 2010

Certified Current 8 August 2012



Communications and Information

**AIR FORCE MATERIEL COMMAND TIER 1
VIDEO TELECONFERENCING (VTC)**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at www.e-publishing.af.mil for downloading or ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: HQ AFMC/A6OK

Certified by: HQ AFMC/ A6O

Supersedes: AFMC PD 33-3,
30 AUGUST 2005

(John Bartoli)

Pages: 14

This instruction prescribes uniform procedures for managing VTC facilities and their maintenance, procedures, and support. The instruction applies to all Tier 1 HQ and Base VTC operations assigned to Air Force Materiel Command. It applies to all other Tier II organizations and contractors residing on an AFMC base or geographically separated unit when conferencing with Tier I facilities. Tier I facilities consist of all primary and alternate sites (dedicated and dial-up) that are used by HQ and field CC, CV, and CDs. Tier II facilities consist of all other AFMC DVS-G registered dial-up sites. This publication does not apply to the Air National Guard (ANG) or to the Air Force Reserve Command (AFRC) and their units. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using Air Force (AF) Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate functional's chain of command. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 33-363, *Management of Records*, and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located in Air Force Records Information Management System (AFRIMS) on the AF Portal: <https://www.my.af.mil/gcss-af61a/afrims/afrims/rims.cfm>

This revision incorporates requirements IAW DODI 8510.01-M, *DOD Information Assurance Certification and Accreditation Process (DIACAP)* and DODI 8500.2, *Information Assurance Implementation*, Attachments A3 and A4 to Enclosure 4, for the AFMC Tier 1 VTC Network.

Chapter 1

VIDEO TELECONFERENCING (VTC).

1.1. HQ AFMC VIDEO TELECONFERENCING (VTC) SUPPORT.

1.1.1. Shall provide the Major Command (MAJCOM) with a VTC Program Management Office (PMO) responsible for all centrally funded video teleconferencing resources in the AFMC VTC Community of Interest (COI).

1.1.2. Shall establish MAJCOM policy and procedures for the AFMC COI.

1.1.3. Shall act as the VTC COI Representative/Network Manager in accordance with Defense Information Systems Agency (DISA) Circular, Jan 98.

1.2. HQ AFMC VTC COI Representative/Program Manager.

1.2.1. Is the single Command focal point and liaison to DISA and the Air Force.

1.2.2. Shall identify requirements and is responsible for acquisition and implementation of Defense Video Services – Global (DVS-G) services for their COI.

1.2.3. Shall assist DISA in developing DVS policies and procedures, Concept of Operations (CONOPS), and evaluation of new technical products.

1.2.4. Shall interpret, disseminate and enforce DOD, Air Force and DVS VTC policy and procedures to all users within the AFMC COI.

1.2.5. Shall develop, implement, and enforce adherence to MAJCOM supplements, policies and procedures.

1.2.6. Shall oversee the overall operational management of AFMC VTC facilities and systems.

1.2.7. Shall monitor, review, and analyze AFMC network performance and ensures effective conflict resolution.

1.2.8. Shall serve as the AFMC COI Contracting Officer's Technical Representative (COTR) for the DISN/DVS-G Network representing AFMC VTC contractual issues and policy for the Command.

1.2.9. Shall conduct inspections and accepts services specified on the DVS-G services contract, and centrally funded VTC maintenance contract.

1.2.10. Shall interface directly with all facility managers and customers to provide policy interpretation and operational and technical guidance.

1.2.11. Shall actively participate in the DISA COI Representative Working Group, DISA VTC Advisory Board, and the Air Force VTC Integrated Process Team (IPT).

1.2.12. Shall serve as the AFMC VTC Configuration Control Board Chairperson. (DCPR-1, Ref DODI 8500.2)

1.2.13. Shall serve as the focal point for all Information Assurance Vulnerability Management (IAVM) issues. (VIVM-1) (Ref DODI 8500.2).

1.3. HQ AFMC VTC Operations.

1.3.1. 88 CG, Wright-Patterson AFB, is the AFMC focal point for scheduling and day-to-day coordination of command-wide reservations.

1.3.2. HQ AFMC/CSR is responsible for the operation and scheduling of the HQ AFMC/CC Situation Room and the AFMC secure VTC Multi-Point Control Unit (MCU). Based on AFMC/CC, CV, and CD's VTC requirements, scheduling of the Situation Room must be cleared through HQ AFMC/CSR.

1.3.3. All VTC's which involve AFMC/CC, CV, or CD (Top 3) must adhere to the following procedures.

1.3.3.1. All Top 3 VTC sessions will be scheduled to start at least 30 minutes before sit-down time. All participating sites will be present and available for AV checks and potential troubleshooting from set-up time to completion of call. A facilitator must be in the facility 30 minutes before conference start time.

1.3.3.2. Facilitators must remain in the room during all Top 3 conferences for the duration of the conference. If directed to leave the room by local participants, a facilitator must remain available directly outside the facility.

1.3.3.3. When scheduling the HQ or the Top 3 Situation Room VTC facilities, enter into the DVS-WS the following statement "NO SPEEDMATCHING – MUST BE ABLE TO TRANSMIT CHARTS".

1.3.3.4. HQ facilitators must have the ability to immediately contact all participating facilitators during VTC's involving the Top 3. Contact must be available either by phone or AF Portal instant messaging capability.

1.4. Base-Level Support for AFMC Field Operations.

1.4.1. Shall provide fully trained facility support manpower to schedule, operate and provide user training.

1.4.2. Shall provide project support personnel to assist with MAJCOM upgrade initiatives.

1.4.3. Shall submit facility changes/enhancement requests to the VTC Network Manager/COTR for approval to ensure system integrity, and AFMC standards and network interoperability are maintained.

1.4.4. Shall provide facility personnel that must be prepared to work flexible hours to meet customer requirements and be available during out of normal duty hours for emergency VTC requirements.

1.4.5. Shall develop a local VTC Customer Guide to aid customers in the development of a successful VTC.

1.4.6. Shall appoint a VTC Communications Security (COMSEC) account custodian to manage VTC COMSEC account in secure facilities.

1.4.7. Shall provide for control of cryptographic hardware and cryptographic key material through the local COMSEC Office.

1.4.8. Shall provide for maintenance of cryptographic equipment provided as Government Furnished Equipment.

1.4.9. Shall direct all unresolved issues, i.e., maintenance contract support, network support, or reservation policy to AFMC VTC Network Manager.

1.4.10. Shall provide an alternate site at each VTC location. Alternate sites have the ability to restore mission support function and strategize recovery plans and procedures. The program includes strategies to recover and perform partial system operations at the alternate facility for an extended period of time. (COAS-1, Ref DODI 8500.2)

1.4.10.1. Shall follow the AFMC VTC Contingency Plan and will coordinate the plan with base level CE offices. Review the AFMC VTC Contingency Plan to ensure the designated alternate sites can support VTC requirements. (CODP-1, Ref DODI 8500.2)

1.4.10.2. Shall perform exercises and drills of the AFMC Contingency Plan annually. Results of the exercise shall be documented in a Memorandum for Record format. (COED-1, Ref DODI 8500.2)

1.4.10.3. Shall comply with the DISA Video Teleconferencing Security Technical Implementation Guide (STIG). (DCBP-1, DCSS-2, ECSC-1, Ref DODI 8500.2)

1.4.10.3.1. Shall comply with the DISA Video Teleconferencing STIG, Chapter 3.9, which requires warning banner be displayed. (ECWM-1, Ref DODI 8500.2)

1.4.10.4. Shall be responsible for annual inventory and validation of VTC hardware. The inventory shall be kept on file locally and updated when hardware changes occur. (DCHW-1, Ref DODI 8500.2)

1.4.10.5. Shall not make any arbitrary changes which may affect the primary system or any interconnected systems. (DCII-1, Ref DODI 8500.2)

1.4.10.6. Shall comply with the Information System Security Policy for AFMC Tier 1 VTC Systems. (VIIR-1, Ref DODI 8500.2)

1.4.10.7. Shall coordinate all Information Assurance Vulnerability Management (IAVM) issues through the AFMC VTC Program Manager. (VIVM, Ref DODI 8500.2)

1.5. VTC Facilitator.

1.5.1. Shall maintain a thorough knowledge and understanding of DOD, DISA, AF, and AFMC VTC policies and procedures.

1.5.2. Shall operate VTC facilities and equipment in accordance with the policies in **1.5.1** as well as other appropriate organizational regulations.

1.5.2.1. Shall complete Defense Information System Network/Defense Video Services-Global (DISN/DVS-G) provided training. DISN/DVS-G offers high quality training for facilitators operating DVS-G facilities. Level 1 training is available on-line at <http://disa.dtic.mil/disnvtc/training.htm> and Level 2 is available at the DISN Video Services Centralized Training Facility. The CTF offers both initial facilitator training (Non-Resident Phase) and an advanced facilitator training (Resident Phase) which will culminate in a facilitator certification. Completion of Level 1 is a mandatory requirement to operate a Tier 1 VTC facility. Level II is preferred but is not mandatory.

- 1.5.3. Shall research availability and schedule all customer required VTC facilities in the automated reservation system.
- 1.5.4. Shall prepare their VTC facility for each individual conference. The facilitator may be required to perform both technical and scheduling functions.
- 1.5.5. Shall be in the VTC facility 30 minutes before the first VTC of the day, 15 minutes before point-to-point VTCs and 30 minutes before multi-point VTCs to assist the network service provider in bringing up the call and be prepared for the video and audio checks performed by the chairing location.
- 1.5.6. Shall perform audio/video checks with each site before customers arrive if they are the chairing site.
- 1.5.7. Shall remain in the facility to operate equipment, assist participants, and troubleshoot possible technical problems when conference is in session.
- 1.5.8. Shall announce to all locations prior to the start of the VTC when the customer has a requirement to video tape an unclassified VTC and will ask if anyone has objections. If one or more locations object, the VTC will not be recorded. Tapes will be furnished by the customer and returned to the customer after VTC ends. (PEDD-1, Ref DODI 8500-2)
- 1.5.9. Shall instruct VTC participants they are required to power off ALL cell phones, Blackberrys, and any other electronic devices/transmitting devices before entering the VTC facility. These devices create audio interference during video conferences for all locations involved in the conference.
- 1.5.10. Shall switch to all locations if they are the chairing facilitator, when participants are talking.
- 1.5.11. Shall provide briefing support to customers. Instruct customers they must brief from the same location where the charts are located.
- 1.5.12. Shall ensure VTC is muted at all times unless customer is speaking. Will instruct audio add-on participants to maintain mute on their phones until they speak.
- 1.5.13. Shall utilize the audio add-on feature when requested and not use local operator assisted meet-me lines due to possible vulnerabilities.
- 1.5.14. Shall enforce command policy on VTC facilities designated as "No Smoking" areas. No food or beverages are permitted in the VTC facility or equipment room(s).
- 1.5.15. Shall not host other sites into a Tier 1 conference using the Coder/Decoder (codec) multisite capability. Sites using this function during a Tier 1 call will be disconnected.

Chapter 2

SECURE VIDEO CONFERENCES AND FACILITIES.

2.1. Management of Secure Video Conferences and Facilities.

2.1.1. All VTC facilitators must understand and use appropriate security guides, such as National Security Telecommunications & Information Systems Security Instruction (NSTISSI) No. 3013 “Operational Security Doctrine for the STU III,” and DISA’s “Key Management Plan for Defense Information System Network Video Services.” (IAKM-3, Ref DODI 8500-2)

2.1.1.1. All system components including encryption devices are determined and controlled by the AFMC VTC CCB. (ECNK-1, Ref DODI 8500.2)

2.1.2. A secure VTC shall not be conducted unless all local security instructions are enforced prior to the start of the VTC sessions. Procedures are documented in the AFMC Daily COMSEC Procedures Guide, dated Sep 09; and in the Information System Security Policy for AFMC Tier 1 VTC Systems, dated Apr 09.

2.1.3. Electronic devices of any type, such as tape recorders, radios, beepers, cell phones, Blackberrys, etc., are not permitted in the VTC room during classified briefings. Battery removal will not suffice, as many electronic devices have an internal battery for memory storage. ALL DEVICES MUST REMAIN OUTSIDE THE FACILITY DURING CLASSIFIED VTCs.

2.1.4. Recording of classified conferences is prohibited. Video Cassette Recorders (VCRs) shall be powered off at the VCR device prior to the start of a classified VTC session. (PECS-2, (PEDD-1, Ref DODI 8500.2)

2.1.5. The loss or compromise of any classified information or keying material at a VTC must be promptly reported through appropriate security channels.

2.1.6. Access Control. The facility is normally comprised of four distinct rooms; the VTC room, the foyer, the equipment room, and the utility (air conditioning/power) room. All of these rooms must be secured while in a secure mode and when the encryption devices are loaded.

2.1.7. A facilitator must remain in the VTC studio when a classified VTC is in session.

2.1.8. Keep the VTC dialogue at or below the level of security classification allowed. Users are fully accountable for what they say and content of visual presentations.

2.1.9. Doors to the VTC studio will be secured when the studios are unattended and during classified conferences.

2.1.10. Only authorized personnel are permitted entry into the VTC equipment room.

2.1.11. Personnel without security clearances must be escorted at all times while in the VTC facility.

2.1.12. No Foreign Nationals shall be granted access to VTC equipment, control units or automated reservation systems. Foreign national participation in a VTC is the responsibility

of the conference chairperson (customer) IAW 2.2.4.1. Foreign National participation shall be IAW Local Foreign Disclosure Office endorsements and need-to-know.

2.2. Secure VTC Setup Procedures.

2.2.1. For point-to-point and multi-point VTCs the connection is established in the secure mode. After secure connectivity is confirmed the facilitator will ensure secure VTC indicator light in the VTC studio is on and also post a sign either on the outside of the VTC facility door, outside of the controlled area, or both, to warn that a secure VTC is in session.

2.2.2. At the VTC chairing location, the conference chairperson (customer) should poll each site to confirm that identities of all participants have been verified and compared against their attendance lists. Attendance lists will be transmitted to other sites by the conference chairperson if required.

2.2.3. The conference chairperson should announce the security level of the meeting prior to starting any discussions.

2.2.4. The conference chairperson who requests a secure VTC (customer) has the overall responsibility for security clearance verification of all attendees prior to the VTC.

2.2.4.1. The VTC conference chairperson ensures that the point of contact at each location obtains the proper clearance verifications for the attendees at their respective locations in accordance with established procedures. The chairperson is responsible for ensuring all participants invited to attend VTC are cleared at the appropriate level when conference is classified. It is not the facilitator's responsibility to maintain clearances on file.

2.2.5. Facilitators must have a security clearance equal to the level of the COMSEC key at the particular facility. Secret is a minimum requirement.

2.3. Physical Security.

2.3.1. Each local organization will ensure their facility meets all local requirements for initially operating at the Secret level.

2.3.2. VTC facilities will not be used to store customer's classified materials. The customer must provide all classified materials required for a VTC and all materials brought in or generated during the VTC must be removed from the facility by the customer immediately following the VTC.

2.3.3. At the end of a classified conference, the facilitator will ensure that the VTC room and equipment is properly sanitized by ensuring removal of all classified materials and rebooting the codec device.

2.3.4. The customer will provide personnel for additional physical security (door guard) during classified conferences.

Chapter 3

AFMC RESERVATION MANAGEMENT.

3.1. AFMC RESERVATION MANAGEMENT PROCEDURES.

3.1.1. The AFMC VTC facilities are available for use by all DOD government organizations on a first come-first serve basis; however, AFMC related VTCs have priority over non-AFMC VTCs.

3.1.2. Customers at the requesting site must have a conference chairperson who will make the reservation request when the need and time for a VTC is determined. The conference chairperson is responsible for organizing, scheduling, and conducting the meetings.

3.1.3. Only the AFMC Commander, Vice Commander, and Executive Director may preempt previously scheduled VTCs. Preemption applies to VTC's where the Commander, Vice Commander or Executive Director physically attend the conference. AFMC field commanders may only preempt previously scheduled VTCs involving their VTC facility. The following sequence applies:

3.1.3.1. The VTC office will notify the preempted conference chairperson. At that time the reservationist will offer another date/time for the conference.

3.1.3.2. The preempted conference chairperson shall notify all participants of the revised schedule.

3.1.4. When using the Defense Video Services Worldwide Scheduling System (DVS-WS), the local reservation office will assist the conference chairperson in choosing available dates and times. When the chairperson selects a preferred time, the reservationists will enter the information in the automated reservation system. A confirmation number confirms each scheduled VTC.

3.1.4.1. The following information from the conference chairperson is required to schedule a VTC:

3.1.4.2. Requested date of conference

3.1.4.3. Time and duration of conference

3.1.4.4. Other locations participating

3.1.4.5. Points of contact with telephone numbers at all locations (customers)

3.1.4.6. Subject of conference

3.1.4.7. Visual presentation requirements

3.1.4.8. Security level of conference

3.1.4.9. Names of participating General Officers

3.1.4.10. The conference chairperson has the responsibility to contact their participants at all locations to inform them of the VTC and shall ensure all participants have need-to-know. (ECAN-1, Ref DODI 8500.2)

- 3.1.5. The conference chairperson has the responsibility to ensure all materials used during VTC are to be marked with appropriate classification level. (ECML-1, Ref DODI 8500.2)
- 3.1.6. Under normal operating conditions, preempting of scheduled VTCs is not permitted. Emergency or high priority situations may arise that will require preempting existing conferences.
- 3.1.7. Changes can only be made to an existing conference by the conference chairperson at the site that initially established the scheduled conference (chairing site).
- 3.1.8. All changes must be made more than 48 hours prior to conference start time. No changes can be made after that time, i.e., adding/dropping sites, extending/changing conference time, etc. Exceptions will be considered for high level, i.e., flag/SES level VTC's only.
- 3.1.9. When cancellations occur, the conference chairperson must provide immediate notification to the reservation office.
- 3.1.9.1. The reservation office shall immediately access the Defense Information Systems Network (DISN) Video Services automated scheduling system and cancel the conference.
- 3.1.9.2. If cancellation occurs within 4 hours of the conference start time, the reservation office shall call the DISN Customer Call Center (DCCC) to cancel.
- 3.1.9.3. The conference chairperson (customer) is responsible for contacting all participants to inform them of the cancellation.
- 3.1.9.4. Frequent "no-shows" by an organization will be documented and may result in monitoring cancellation of future requirements.
- 3.1.10. Normal operating hours for each facility is 0730–1700 but will vary depending on the respective time zones.
- 3.1.11. The AFMC Tier 1 VTC Network is communications support for day-to-day business and under no circumstances will be scheduled for training of any kind.
- 3.1.12. The AFMC Tier 1 VTC facilities are to be used for official video conferencing and will not be used as a regular conference room for non-VTC meetings.
- 3.1.13. During normal duty hours, base-level reservation desks must be manned at all times. If manning shortages prevent this, voice mail should be provided with a pager number or cell phone number where the facilitator can be reached immediately.
- 3.1.14. Information concerning scheduled VTCs is considered privileged information and will not be given to anyone other than the known participants.
- 3.1.15. Organizations will not forfeit confirmed conference timeslots to other organizations unless coordinated with the VTC office.
- 3.1.16. All VTC's will be scheduled at a minimum operating bandwidth of 384 Kbps.
- 3.1.17. All VTC's which involve the HQ Tier I facilities and which are scheduled by an AFMC VTC location, shall not be scheduled using any organizationally owned MCU's

without VTC Network Manager authorization. Organizationally owned MCU's may introduce risk of non-DVS-G sites into conference.

3.1.18. A VTC can be scheduled at quarter hour intervals, i.e., on the quarter hour, half hour, three quarter hour or hour but will be limited to 2 hours.

3.1.19. AFMC will accept reservations for regularly scheduled VTCs (i.e., weekly, monthly, and quarterly). Requests for regularly scheduled VTCs will be submitted in writing or by e-mail with required information.

3.1.20. Reservations can be made up to 6 months in advance.

3.1.21. When dialing an ISDN number, use DSN, not commercial long distance carriers, to call other DOD activities unless DSN service is not available in a timely manner. DSN is the first choice for ISDN dialing requirements if available.

3.1.22. All scheduled VTCs must be initiated by a government organization. Contractors in support of their contract may schedule a VTC, but must be sponsored by a government organization.

3.1.23. Some codecs have a Multisite option enabling you to bring in other sites through your codec. This option is not authorized and cannot be used to "host" any other sites into a Tier 1 call. Ensure codec settings are adjusted accordingly so that Multisite does not automatically take calls without facilitator control/approval. Sites using this function during a Tier 1 call will be disconnected.

Chapter 4

COMMUNICATIONS SECURITY (COMSEC).

4.1. COMMUNICATIONS SECURITY (COMSEC) Management.

4.1.1. DISA is the controlling authority for all DOD VTC keying materials for the KIV-7 encryption device. Keying material is assigned to the local COMSEC account.

4.1.2. Keying material will be authorized by DISA and the National Security Agency (NSA), after the facility has been certified and accredited by the AF Designated Approval Authority (DAA).

4.1.3. Keying material will be maintained by either the local VTC facilitator or the local COMSEC Responsible Officer (CRO) who will be responsible for its security.

4.1.4. When the encryption device is keyed, the CRO or VTC facilitator must be physically present within the security perimeter of the VTC room at all times.

4.1.5. Encryption equipment at each facility is assigned to the local organization's equipment account and the keying material (keymat) is assigned to the local COMSEC account.

4.1.6. Encryption devices shall be loaded in accordance with DISA procedures. These procedures can be located on the DISA VTC website at <https://dvsops.scott.disa.mil/dvsws>.

4.1.7. Recovery of encryption configuration settings can be found in the AFMC COMSEC Daily Procedures Guide (COTR-1, Ref DODI 8500.2)

Chapter 5

VTC FACILITY.

5.1. VTC FACILITY MAINTENANCE.

5.1.1. VTC facilitators are required to report all maintenance problems to the contracted maintenance provider in accordance with established procedures.

5.1.1.1. Facilitators should receive appropriate trouble ticket number from maintenance contractor so trouble can be tracked.

5.1.2. Facilitators are required to obtain approval from AFMC DVS-G Network Manager before pulling from spare parts on large ticket items.

5.1.3. VTC facilitators are required to provide limited technical support to analyze and isolate equipment problems.

5.1.4. When loss of codec software occurs, VTC facilitators are required to contact the AFMC VTC Program Management Office /AFMC VTC CCB Chairperson. (DCSW-1, Ref DODI 8500.2) The AFMC maintenance provider is the only authorized personnel permitted to download upgrades from manufacturer's website for upgrades and software backup. (COSW-1, DCCT-1, Ref DODI 8500.2) Backup and restoration assets for the VTC systems consist of the codec and MCU settings and are maintained and protected at an off-site location by the contract maintenance provider. (COBR-1, Ref DODI 8500.2)

5.1.5. AFMC VTC equipment maintenance is provided by contracted/authorized personnel only.

5.1.6. Personnel performing maintenance must provide the information necessary to the VTC facilitator so they can prepare the Visitors Request Form located on the AF Portal. The Visitors Request Form shall be kept on file locally at each location. (PRMP-2, Ref DODI 8500.2)

5.1.6.1. Escorted access shall be IAW *AFMC Communications Security (COMSEC) Daily Procedures*, Chapter 2.3.2. "All visiting individuals must be signed in on an AF Fm 1109". (PRMP-2, Ref DODI 8500.2)

5.1.6.2. Contractor personnel shall be escorted when on-site to perform equipment maintenance. (PRMP-2, Ref DODI 8500.2)

Chapter 6

ENVIRONMENTAL CONTROLS.

6.1. ENVIRONMENTAL CONTROLS.

6.1.1. Battery operated or electric stand-alone smoke detectors shall be installed. Smoke detectors shall tested when universal time changes occur. (PEFD-1, Ref DODI 8500.2)

6.1.2. VTC facilities shall undergo a periodic fire marshall inspections, in accordance with building fire codes and regulations. Deficiencies are promptly resolved. (PEFI-1, DODI 8500.2)

6.1.3. Handheld fire extinguishers or fixed fire hoses shall be available should an alarm be sounded or a fire be detected. (PEFS-1, Ref DODI 8500.2)

6.1.4. Each facility shall conduct an annual penetration test. Testing shall include unannounced attempts to penetrate VTC equipment rooms. Testing shall be documented and kept on file at each location. (PEPS-1, Ref DODI 8500.2)

Chapter 7**PRESCRIBED FORMS**

7.1. Prescribed Forms Form prescribed is AF IMT Form 1109, *Visitor Register Log*.

TIMOTHY K. BRIDGES, SES
Director of Communications
Installations and Mission Support