



DEPARTMENT OF THE ARMY  
OFFICE OF THE SECRETARY OF THE ARMY  
107 ARMY PENTAGON  
WASHINGTON DC 20310-0107

Office, Chief Information Officer/G-6

S: 30 September 2015

SAIS-PRU

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Video Teleconference (VTC) Modernization Policy and Reporting Guidance

1. References:

- a. Army Regulation (AR) 25-13, Telecommunications and Unified Capabilities, 25 March 2013.
- b. AR 25-1, Army Information Technology, 25 June 2013.
- c. AR 25-2, Information Assurance, 23 March 2009.
- d. Department of Defense Directive 8570.01, Information Assurance (IA) Training, Certification, and Workforce Management, 15 August 2004.
- e. Department of Defense Instruction 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), 12 March 2014.
- f. Headquarters, Department of the Army General Order 2014-02, 6 March 2014.
- g. Defense Information Systems Agency (DISA) Network Services Directorate Enterprise Connection Division Defense Information Systems Network (DISN) Connection Process Guide, November 2013.
- h. Memorandum, Director, DISA, 14 July 2014, subject: Defense Information Systems Network (DISN) Sunset of Legacy Systems.
- i. Memorandum, Army Chief Information Officer/G-6, 21 August 2014, subject: Secure Use of Army Video Teleconference (VTC) Capabilities.

2. Purpose. To provide interim policy guidance for the Army's management of VTC equipment connected to the Army's unclassified and classified networks in order to improve service, reliability, performance and user experience.

SAIS-PRU

SUBJECT: Video Teleconference (VTC) Modernization Policy and Reporting Guidance

3. Policy Guidance.

a. Army Commands, Army Service Component Commands, Direct Reporting Units, the Army National Guard/Army National Guard of the United States and the U.S. Army Reserve will:

1) Migrate VTC services from Integrated Services Digital Network (ISDN) to Internet Protocol (IP) technology no later than 30 September 2015.

a) Commands unable to meet the suspense date for this requirement will report to Second Army every 90 days (see paragraph 3.a.7 and Enclosure 2) until the migration is complete. Commands that fail to meet the suspense date for migration will receive a recurring bill for ISDN services from DISA, in accordance with reference 1h (see Enclosure 3).

b) Where Multi-Protocol Label Switching (MPLS) cannot satisfy the VTC requirement, ISDN gateway services will be offered. A waiver must be approved by CIO/G-6 (via the Information Technology Approval System) prior to procuring these ISDN services.

2) Purchase IP transport rather than ISDN transport for any new or refreshed systems after the date of signature on this memorandum.

3) Ensure that all personnel are informed of VTC etiquette and best practices (see Enclosure 1).

4) Identify a point of contact in the rank of at least Colonel or GS-15 on the template at Enclosure 2.

5) Ensure that all hardware and software supporting VTC solutions or services are reported in the Army Portfolio Management Solution (APMS). APMS information can be located at <https://www.eprobe.army.mil/enterprise-portal/web/apms/home>.

6) Reduce the use of Multi-Point Control Units (MCUs) to the minimum amount possible, which is important in maintaining optimum performance of VTC services. Commanders and agency and organization chiefs will ensure that end points and MCUs connect directly to the host end point or MCU without cascading or daisy-chaining.

7) Report all VTC systems to [usarmy.huachuca.hqda-netcom-ncr.mbx.enterprise-vtc-group@mail.mil](mailto:usarmy.huachuca.hqda-netcom-ncr.mbx.enterprise-vtc-group@mail.mil).

SAIS-PRU

SUBJECT: Video Teleconference (VTC) Modernization Policy and Reporting Guidance

a) This annual reporting mechanism will provide a current inventory of baseline and mission-supported VTC capabilities and resources.

b) Submitted reports will provide metrics, detailed system information and growth requirements to assist with Wide Area Network capacity management, quality-of-service settings, life-cycle replacement and integration with ongoing network modernization initiatives, such as implementation of Joint Regional Security Stacks (JRSS), MPLS and Unified Capabilities.

b. Second Army will monitor Army network traffic to enforce security regulations and policies for VTC services. Second Army will discontinue network availability of circuits to Commands that are not in compliance.

c. VTC system owners, administrators and managers will:

1) Validate that personnel with elevated access to VTC systems have completed appropriate computing environment training certifications and qualifications, including:

a) Online DISA Global Video Services Facilitator and User VTC certification courses/modules, which can be found at <https://disa.deps.mil/ext/COP/NS-Extranet/ExternalConnect/SitePages/Home.aspx>.

b) Army-specific training appropriate for hardware and software in use at the location.

c) Vendor-specific training appropriate for hardware and software in use at the location.

d) Facilitator and user training as published by CIO/G-6 (SAIS-PRU).

2) Provide all users a basic understanding of recommended VTC etiquette and best practices (see Enclosure 1). Commands may strengthen these practices by adding additional standards and practices particular to their environment.

3) Implement and enforce the use of all applicable standard operating procedures, checklists, configurations and tactics, techniques and procedures for VTC infrastructure, conference rooms and personnel.

4) Ensure that VTC systems are, or will be, connected via IP network in accordance with references a, c and g. Connected systems must meet Department of Defense, DISA and Army requirements for operating on the IP network. Systems must

SAIS-PRU

SUBJECT: Video Teleconference (VTC) Modernization Policy and Reporting Guidance

be validated by the local Network Enterprise Center, authorized designee or Network Operations Center prior to connecting to the network.

5) Ensure that all VTC equipment and services are sustained and appropriately supported with secure system configurations and security patches in accordance with references c, g, h and i in order to connect or remain connected to the Department of Defense Information Network and LandWarNet.

4. Expiration. This policy guidance will remain in effect until incorporated into Army Regulation 25-13.

5. Points of contact: Ms. Asmayit Yohannes, (703) 697-9061 (DSN 865) or [asmayit.a.yohannes.civ@mail.mil](mailto:asmayit.a.yohannes.civ@mail.mil); and Mr. Kai Beasley, (703) 545-1572 (DSN 865) or [kai.a.beasley2.ctr@mail.mil](mailto:kai.a.beasley2.ctr@mail.mil).

Encls

ROBERT S. FERRELL  
Lieutenant General, GS  
Chief Information Officer/G-6

DISTRIBUTION:

Principal Officials of Headquarters, Department of the Army  
Commander

- U.S. Army Forces Command
  - U.S. Army Training and Doctrine Command
  - U.S. Army Materiel Command
  - U.S. Army Pacific
  - U.S. Army Europe
  - U.S. Army Central
  - U.S. Army North
  - U.S. Army South
  - U.S. Army Africa/Southern European Task Force
  - U.S. Army Special Operations Command
  - Military Surface Deployment and Distribution Command
  - U.S. Army Space and Missile Defense Command/Army Forces Strategic Command
  - U.S. Army Medical Command
  - U.S. Army Intelligence and Security Command
  - U.S. Army Criminal Investigation Command
- (CONT)

DISTRIBUTION (CONT):

U.S. Army Corps of Engineers  
U.S. Military District of Washington  
U.S. Army Test and Evaluation Command  
U.S. Army Installation Management Command  
Superintendent, U.S. Military Academy  
Director, U.S. Army Acquisition Support Center  
Executive Director, Arlington National Cemetery  
Commander, U.S. Army Accessions Support Brigade  
Commandant, U.S. Army War College  
Commander, Second Army

CF:

Director, Army National Guard  
Director of Business Transformation  
Commander, Eighth Army  
Commander, U.S. Army Cyber Command