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

Office, Chief Information Officer/G-6

SAIS-CB

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Secure Use of Army Video Teleconference (VTC) Capabilities

1. References.

a. Army Regulation (AR) 25-2, Information Assurance (IA), 23 March 2009.

b. AR 25-1, Army Information Technology (IT), 25 June 2013.

c. AR 25-13, Telecommunications and Unified Capabilities, 25 March 2013.

d. AR 380-5, Department of the Army Information Security Program, 29 September 2000.

e. AR 190-13, The Army Physical Security Program, 25 February 2011.

f. Department of the Army Pamphlet (DA PAM) 25-1-1, Army Information Technology Implementation Instructions, 25 June 2013.

g. Defense Information Systems Agency (DISA) Video Tele-Conference Security Technical Implementation Guide (STIG), 27 February 2014.

2. Purpose. This memorandum clarifies Army policy associated with the installation and operation of unclassified and classified VTC capabilities. Examples of VTC capabilities include, but are not limited to: conference room audio/video systems; desktop VTC implementations; webcams; and cameras on devices, to include mobile devices. The risks introduced by VTC capabilities include, but are not limited to: unauthorized disclosure of classified information; unauthorized disclosure of sensitive information (e.g., Privacy Act, For Official Use Only, Controlled Unclassified Information); covert and overt monitoring (e.g., compromised systems, unauthorized attendees, overheard discussions); and unauthorized or improper use.

3. Applicability. The policy in this memorandum applies to the active Army, the Army National Guard / Army National Guard of the United States, and the U.S. Army Reserve.

4. Policy.

a. Usage.

1) It is the responsibility of all personnel with access to unclassified or classified VTC capabilities to ensure and promote their secure use. Failure to use these capabilities securely may result in disciplinary action, in accordance with applicable laws and regulations.

2) Only use VTC capabilities with official services and for official purposes. This includes authorized Family and Morale, Welfare and Recreation activities.

3) Promptly report any unauthorized or improper use of VTC capabilities to the local Information Assurance Manager, Security Manager or Physical Security Officer.

4) Remove from the camera field of view or fully cover sensitive and classified information that is not part of the VTC, accounting for cameras with hardware or software-based pan and zoom capabilities. This includes moving, fully covering or powering off displays that either show such information or have a classification marking that may give the impression that information inappropriate to the VTC may be shown.

5) Use headsets, headphones, device handsets, close-range microphones, highly-directional microphones and/or reduced microphone gain for VTC audio.

6) Mute microphones when not speaking.

7) When a VTC is not in use:

i. Power off, de-activate or disable webcams and cameras on devices.

ii. Power off, de-activate or disable cameras and microphones.

iii. Power off, de-activate, disable or disconnect dedicated VTC equipment.

iv. Cover the camera lens and/or point cameras to a wall, corner or ceiling where room activities and sensitive or classified information are not visible.

b. Implementation.

1) When implementing unclassified or classified VTC capabilities, follow all applicable policy and procedures; secure the capbilities per the most recent DISA STIGs applicable to the VTC technology, connectivity, software and hardware; and

ensure that the capabilities are maintained with security-related patches and security-related firmware updates.

2) Incorporate policy and procedures for the secure use of authorized VTC capabilities within user agreements and Installation Security Plans.

3) Change any default passwords to unique passwords that are STIG-compliant.

4) The Network Enterprise Center (NEC) or designated IT provider must approve all VTC systems and implementations.

5) For either unclassified or classified VTC capabilities, to include webcams and cameras on devices, within areas designated as classified, secure, restricted, open storage or closed storage:

i. A signed authorization (written or email) must be obtained by the Garrison Commander or tactical equivalent for VTC capability use within these areas; and

ii. Signed authorization (written or email) must also be obtained from the appointed Authorizing Official (AO)/Designated Approving Authority (DAA) of the Army Signal Command (Theater) or other area of responsibility in order for the VTC capability to connect to one or more systems or networks.

6) The areas requiring the above authorizations include, but are not limited to: those in which classified information is approved for discussion, storage, processing or transmission; mission-essential vulnerable areas; and staging areas before deployment.

7) The NEC or designated IT provider will maintain a record of both the Garrison Commander, or tactical equivalent, and the AO/DAA authorizations.

8) Authorizations will expire upon expiration of the accreditation for the specific VTC system/implementation; or upon expiration of an accreditation in which the VTC capabilities are integrated, such as for a system or network. New authorizations are required for significant changes to hardware, software, locations and/or connectivity.

5. Exceptions. Approval of exceptions to specific policy, procedures and guidance (e.g., reference g) may only be granted (written or email) by the appointed AO/DAA of the Army Signal Command (Theater) or other area of responsibility in order to meet compelling mission-essential operational requirements. Exceptions must be documented in the Plan of Action and Milestones (POA&M) maintained with the system/network accreditation.

6. Compliance. Current VTC capabilities, to include webcams and cameras on

devices, that are operating without proper approval and authorizations (paragraph 4b) or are non-compliant with this policy (paragraph 4) must request approval, authorization and any necessary exceptions within 30 days of publication of this memorandum.

7. Enforcement. Commanders, leaders and AOs/DAAs will ensure enforcement of this policy. Effectiveness will be determined by Cyber Security/Information Assurance compliance assessments and the applicable POA&M. This policy will be reviewed for update annually.

8. The point of contact for this memorandum is Ms. Melissa Hicks, CIO/G-6 Cyber Security Directorate: melissa.c.hicks.civ@mail.mil or (703) 545-1604.

FERRELL.ROBERT.SILAS.1028607268
Digitally signed by FERRELL.ROBERT.SILAS.1028607268
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USA, cn=FERRELL.ROBERT.SILAS.1028607268
Date: 2014.08.21 15:58:47 -04'00'

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 Strategic Command
- U.S. Army Medical Command
- U.S. Army Intelligence and Security Command
- U.S. Army Criminal Investigation Command
- U.S. Army Corps of Engineers
- U.S. Army Military District of Washington
- U.S. Army Test and Evaluation Command
- U.S. Army Installation Management Command

Superintendent, United States Military Academy
(CONT)

DISTRIBUTION (CONT):
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