

## ANNEX F

### (U) CONNECTION APPROVAL PROCESS (CAP) FOR SECURE TERMINALS

1. **Introduction** - This annex addresses specific connection requirements for secure terminals to operate on the Defense Information System Network (DISN) Video Services (DVS) Network. The major components of this process are:

- An objective evaluation of customer documentation to determine if customer documentation meets security criteria;
- A system verification testing activity; and
- A database to manage and provide status information on the approval process;

2. **DVS** - DVS is the video transfer portion of the DISN. It supports controlled, UNCLASSIFIED through SECRET video teleconferences, on a worldwide basis. The connection requirements defined below must be met before video teleconferences are allowed.

3. **DVS Registration** – All DVS customer sites must be registered with DISN Video Services. All non-DoD organizations must be sponsored by a DoD organization prior to their registration being accepted. A copy of the sponsorship letter between the non-DoD organization must be submitted to DISA DISN Video Services (GS25) with the CAP documentation.

4. **Initial Contact.** All customers desiring connection to DVS must first contact the appropriate DVS Account Manager (AM). Identification and telephone number of the AM assigned to each Service, Department, Agency, or theater can be obtained by contacting DISN's Video Services Division, GS25 at DSN 312-761-4111 or COML 703-681-4111.

5. **DVS System Security Package.** Each customer requiring video services connectivity must submit an Approval to Operate (ATO) or Interim Approval to Operate (IATO) letter from the cognizant Designated Approving Authority (DAA) to DISA DISN Video Services (GS25).

a. **ATO** - Each ATO letter must identify the mode(s) of operation, the highest classification level of information being processed, and any residual security risks that are not mitigated. A sample accreditation letter is attached as Enclosure 1.

b. **IATO** - If the system is not fully accredited, the cognizant DAA may submit an IATO stating that he/she accepts all significant risks under which the Video Teleconferencing Facility (VTF) is currently operating. This letter must also identify the mode(s) of operation, the highest classification level of information being processed, any risks that preclude accreditation, and any ongoing or planned actions to mitigate those risks. Due to the length of time it takes to process new sites for keying material an IATO will not be accepted for less than 90 days. An IATO may be submitted for the maximum time of one year IAW DODI 5200.40. If an ATO is not completed after the one year IATO a 90 day IATO may be submitted while the ATO is being processed. After 15 months of operation with an IATO the site will be suspended until an ATO is received. A sample IATO letter is attached as Enclosure 2.

**6. VTF Connectivity Diagram** - This diagram identifies all components and system connections in the VTF. It must address both direct and backside connections, to include the customer's MCU connections to other MCUs or VTFs directly or indirectly. It must also identify connections to other video, voice, or data networks. The VTF connectivity diagram must also include all associated devices including video equipment, MCUs, line interface units (LIUs), hubs, routers, guards, firewalls, gateways, modems, encryption devices, and backup devices.

**7. Consent to DISA Monitoring & Compliance Assessment** - ATO and IATO letters must be signed by a DAA and must include the following statement: "We acknowledge and consent to DISA conducting an initial vulnerability assessment and periodic, unannounced vulnerability assessments on the connected host systems, to determine the security features in place to protect against unauthorized access or attack."

**8. Automated Information System (AIS) Concept of Operations (CONOPS), Security CONOPS, Security Standard Operating Procedures (SOP)** - These security documents must describe how administrative security, procedural security, personnel security, and physical security requirements are implemented in the VTF environment. They must also identify the data types and classification level of the VTF owner and its cognizant DAA. Where appropriate, customer procedures must describe how the VTF and video equipment performs periodic processing to transfers between different call classification levels.

**9. Allied Connection Access Policy** - DVS provides video services at Controlled UNCLASSIFIED, US-Only SECRET, US-Only SECRET, and Allied SECRET. Connections to elements of foreign governments are permissible when the Commander, as the sponsoring activity, provides an ATO that identifies the connection and accepts the risk. Connections to foreign subscriber terminals must be made through the use of approved security devices employed at each foreign connection.

**10. External Connections** - A copy of each external connection and/or associated operation agreement affecting the applying VTF must be provided in the form of a Memoranda of Agreement/Understanding (MOA/MOU). If no external connections apply, ATO and IATO letters must contain statements of non-applicability. Direct DVS subscribers are responsible for ensuring that all backside connections comply with DVS standards. Where external connections introduce unacceptable risk to the DVS Network, DISA may withhold connection authority, pending a decision by the DISN Security Accreditation Working Group/Joint Staff (DSAWG/JS).

**11. Exercises.** Commanders who require DVS subscriber terminals to support an exercise must provide the above information at least 60 days prior to its scheduled commencement.

**12. COMSEC Key** - DVS subscribers are required to coordinate with their supporting COMSEC custodians/managers to ensure that DISA GS25 authorizes issue of required KG-194/KIV-19 or KIV-7HS keys.

**13. Processing DVS Packages** - After all required information has been submitted to the DISN Video Services Division (GS25), each DVS request package will be reviewed, entered into the Video Services database, and forwarded to the DVS Contractor for continued processing.

**14. Reporting System Changes** - When any significant change is made to a DVS VTF terminal affecting environment, accreditation status, security posture, foreign access, and/or backdoor/backside connectivity, the responsible commander must submit appropriate information to DISN Video Services (GS25).

15. **DVS Termination.** DISA DISN Video Services (GS25) reserves the right to deny or discontinue DVS access to any network, system, or terminal demonstrating behavior that increases risk to the DISN infrastructure and/or its subscribers and for non-compliance with the DVS connection requirements.

a. **Risk Review**- Any DVS connection that introduces unacceptable risk must be reviewed by the DSAWG, which may be contacted via a Service/Department/Agency point of contacts. Combatant Commander may contact the DSAWG via the Joint Staff.

b. **User Notification** - Commanders responsible for DVS terminals that exhibit unacceptable risk will be notified by the Chief, DISN Video Services.

16. **Security Awareness & Training** - Each DVS customer must have an active security awareness and training program for all terminal users, system and security administrators, and managers. Security training and awareness programs must be conducted according to guidance applicable to the local support unit and, at a minimum, the requirement of Section 5 (Federal Computer System Security Training) of Public Law 100-235, the **Computer Security Act of 1987**.

17. **Insecurity Incident Reporting** - Each DVS customer must be capable of detecting unauthorized activity and must have effective procedures for responding to discovered insecurity incidents. Each DVS ST must also have procedures for responding to discovered insecurity incidents detected through audit data reviews, such as break-ins at DVS terminals, viruses, Trojan horses, and other attacks, such as flooding and protocol spoofing. DVS subscribers must also remain current with respect to security patches and updates, in accordance with established Information Assurance Vulnerability Assessment Program that apply to the DISN connection security device and must maintain a secure configuration management environment.

18. **Site Inspections** – Under authority granted by the U.S. Military Communications Electronics Board, DISA DISN Video Services (GS25) reserves the right to conduct announced site compliance inspections of DVS terminals. Responsible commanders will be notified at least two weeks prior to each such inspection.

19. **Re-certification & Approval** - Re-certification of all VTC systems connected to DVS is required every three years, for sites operating under ATOs, and every year for those sites operating under IATOs. This complies with policies stated in DoDD 8500.1, **Information Assurance (IA)**, dated 24 October 2002, and DoDD 8500.2 **Information Assurance (IA) Implementation**, dated 6 February 2003, and as prescribed by DoD 5200.40, **Department of Defense Information Technology Security Certification and Accreditation (C&A) Process (DITSCAP)**, dated 30 December 1997. Re-certification letters will be forwarded to the DISN Video Services' division, GS25.

20. **Requests for Service** - DVS customers must submit Request for Service (RFS) letters to their supporting Telecommunications Certification Office (TCO) for issuance of Telecommunications Service Requests (TSRs), in accordance with DISA Circular (DISAC) 310-130-1, **Submission of Telecommunications Service Requests**, dated 4 April 2000.

21. **DVS Points of Contact** – The following list of positions assigned to the DVS Video Services Division is provided for the convenience of DVS customers:

UNCLASSIFIED

<b>Position</b>	<b>Commercial Phone</b>	<b>DSN (312)</b>
COMSEC Controlling Authority/IA Officer	703-882-0501	381-0501
Chief, DVS	703-882-0049	381-0049
Site Registration	703-681-4111	761-4111
VNMC, Dranesville, VA	1-800-367-8722	533-3000
DISN Customer Call Center - DVS	1-800-554-3476	850-4790
Account Manager: Army, Pacific, STEP	703-681-3847	761-3847
Account Manager: Air Force, Europe	703-681-4106	761-4106
Account Manager: Navy, Marines, USCG	703-681-4110	761-4110
Account Manager: Non-DoD, DISA	703-681-3813	761-3813
Account Manager: COCOMs	703-681-3788	761-3788
Current Operations	703-882-0112	381-0112
Pacific Operations	808-656-0196	315-456-0196
European Operations	011-49-711-686395840	314-434-5840

Encls:

1. - Sample Authorization to Operate Memorandum
2. - Sample Interim Authorization to Operate Memorandum

ENCLOSURE 1

SAMPLE AUTHORIZATION TO OPERATE MEMORANDUM

Commander/Service/Department/Agency  
Letterhead

(Date)

MEMORANDUM FOR: Director, Defense Information Systems Agency ATTN: GS25

SUBJECT: Authorization To Operate a Defense Information System Network (DISN)  
Video Services (DVS) Subscriber Terminal (or system)

REFERENCE: (a) (Command/Service/Department/Agency) Security regulation /Instruction  
XXX-XXX, Subject: ---, dated ----.

(b) DoD 5200.40 - DoD Information Technology Security Certification and Accreditation  
Process (DITSCAP), December 30, 1997 (or Interim DIACAP Guidance Dated 06 July  
2006).

**(NOTE: The references shown above are a minimum listing. An Authority To Operate should include all references cited in your System Security Authorization Agreement, or Certification and Accreditation documentation. Remove this note when drafting your DVS Site's ATO.)**

1. In accordance with provisions of reference (a), authorization is hereby granted for operation of a DVS subscriber terminal (or system) supporting (Command/Element Name) located at (address, building and suite/room). This accreditation is based on a review of the information provided in reference (b). It is only valid if the Baseline Security Safeguards defined in the (Commander/Service/ Department/Agency) specific security guidelines are implemented at the named DVS terminal (or system). That terminal (or system) is authorized to operate in the threat environment defined in reference (b) and with the vulnerabilities identified in applicable (Commander/Service/Department/ Agency) Baseline Security documents. The accredited terminal (or system) consists of (list equipment). It is authorized to process information classified (specify maximum classification) and below. The named terminal (or system) is connected to DVS and (name any other network(s) to which the terminal is connected).

2. This authorization is valid for three years from the date of this memorandum. Reaccreditation/re-authorization is required sooner if there are any significant changes that affect the security posture of the terminal (or system). It is the responsibility of the commander or senior official in charge of the terminal (or system) to ensure that any change in threat, vulnerability, configuration, hardware, software, or connectivity or other modification is analyzed to determine its impact of terminal (or system) security. Appropriate safeguards will be implemented to maintain a level of security commensurate with the requirements of this accreditation.

3. The undersigned accepts the risk for the operation of the system defined above. "We acknowledge and consent to DISA conducting an initial vulnerability assessment and periodic, unannounced vulnerability assessments on the connected host systems, to determine the security features in place to protect against unauthorized access or attack."

/s/ (original signature)  
Commander/Director/Service/Department/Agency  
Designated Approving Authority

Copy to: (Commander/Official responsible for operating the named terminal [or system])

**ENCLOSURE 2**

**SAMPLE INTERIM APPROVAL TO OPERATE MEMORANDUM**

Commander/Service/Department/Agency  
Letterhead

(Date)

MEMORANDUM FOR: Director, Defense Information Systems Agency ATTN: GS25

SUBJECT: Interim Approval to Operate Defense Information Network (DISN)  
Video Services (DVS) Subscriber Terminal (or System)

REFERENCE: (a) (Command/Service/Department/Agency) Security regulation /Instruct  
XXX-XXX, Subject: ---, dated ----.

(b) DoD 5200.40 - DoD Information Technology Security Certification and  
Accreditation Process (DITSCAP), December 30, 1997 (or Interim DIACAP Guidance  
Dated 06 July 2006).

**(NOTE: The references shown above are a minimum listing. An Interim Authority To Operate should include all references cited in your System Security Authorization Agreement, or Certification and Accreditation documentation. Remove this note when drafting your DVS Site's IATO.)**

1. In accordance with the provisions of the reference (a), an Interim Approval to Operate (IATO) is hereby granted to operate a DVS subscriber terminal (or system) supporting (Command/Element Name), located in (address, building, and suite/room). This IATO is based on a review of the information provided in reference (b). It is only valid if the Baseline Security safeguards defined in (Commander/Service/Department/Agency) are implemented at the named DVS terminal (or system). That terminal (or system) is authorized to operate in the threat environment defined in reference (b) and with the vulnerabilities identified in applicable (Commander/Service/Department/Agency) Baseline Security documents. The named terminal (or system) consists of the following (equipment list). It is authorized to process information (specify maximum classification) and below. The named terminal (or system) is connected to the DVS and (name any other network(s) to which the terminal is connected).

2. This IATO is valid for **xxx days** or **1 year** from the date of this memorandum. It terminates sooner, if there is any change that affects the security posture of the terminal (or system). Final accreditation action is required before the expiration of this IATO. It is the responsibility of the commander or senior official in charge of the terminal (or system) to ensure that any changes in threat, vulnerability, configuration, hardware, software, or connectivity or other modification is analyzed to determine its impact on terminal (or system) security. Appropriate safeguards will be implemented to maintain a level of security consistent with the requirements of this IATO.

3. The undersigned accepts the risk for the operation of the system defined above. "We acknowledge and consent to DISA conducting an initial vulnerability assessment and periodic, unannounced vulnerability assessments on the connected host systems, to determine the security features in place to protect against unauthorized access or attack."

/s/ (original signature)  
Commander/Director/Service/Department/Agency  
Designated Approving Authority

Copy to: (Commander/Official responsible for operating the named terminal [or system])