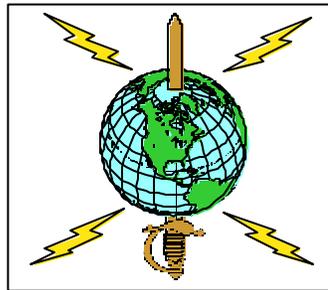


MULTINATIONAL VIDEOCONFERENCING SERVICES

ACP 220



JUNE 2003

FOREWORD

1. ACP 220, MULTINATIONAL VIDEOCONFERENCING SERVICES, is an UNCLASSIFIED Allied Communication Publication (ACP). Periodic accounting is not required.
2. ACP 220 is effective for National, Service or Allied use WHEN DIRECTED.
3. This publication contains Allied military information and is furnished for official purposes only.
4. It is permitted to copy or make extracts from this publication without consultation with the Combined Communications Electronics Board.

**THE COMBINED COMMUNICATION-ELECTRONICS BOARD
LETTER OF PROMULGATION
FOR ACP 220**

1. The purpose of this Combined Communication Electronics Board (CCEB) Letter of Promulgation is to implement ACP 220, VIDEOCONFERENCING SERVICES within the Armed Forces of the CCEB Nations. ACP 220, is an UNCLASSIFIED publication developed for Allied use and under the direction of the CCEB Principals. It is promulgated for guidance, information, and use by the Armed Forces and other users of military communications facilities.
2. ACP 220 is EFFECTIVE ON RECEIPT. The status of this publication is shown below.

EFFECTIVE STATUS

Publication	Effective for	Date	Authority
ACP 220	CCEB	On Receipt	COMAG 03-02

3. Service-originated correspondence will be forwarded through the normal military chain of command, marked for the attention of the appropriate Service communications chief or director. All proposed amendments to the publication are to be forwarded to the national co-ordinating authorities of the CCEB.

For the CCEB Principals:

N. A. Cram
Squadron Leader
Permanent Secretary of the CCEB

TABLE OF CONTENTS

Title Page.....	I
Foreword.....	II
Letter of Promulgation.....	III
Record of Message Corrections.....	IV

Chapter 1**General Information**

101. Purpose.....	1-1
102. General.....	1-1
103. Overview of Multinational Videoconferencing Services.....	1-1
104. Duties and Responsibilities.....	1-2
105. Concept of Operations.....	1-5
106. Liaison.....	1-6
107. Access to Facilities.....	1-6

Chapter 2**Interoperability Requirements**

201. General.....	2-1
-------------------	-----

Chapter 3**Secure Videoconferencing Services**

301. General.....	3-1
302. MSAB Procedures.....	3-1
303. Key Material Management.....	3-2
304. Reporting Loss or Compromise of Keying Material.....	3-4
305. Security Procedures.....	3-4
306. Exchange and Use of Information.....	3-5
307. Controlled Unclassified Information.....	3-5

Chapter 4**Glossary of Terms**

401. Terms used in this Publication.....	4-1
--	-----

Annex A

Australian Defence Videoconferencing Network..... A-1

Appendix A1

How to Conduct a Successful VTC..... A1-1

Annex B

Canadian Videoconferencing Network..... B-1

Annex C

New Zealand Defence Force Videoconferencing Network..... C-1

Annex D

United Kingdom’s Videoconferencing Network..... D-1

Annex E

United States Video Conferencing Network..... E-1

List of Effective Pages

List Of Effective Pages LEP-1

List of Tables

Table 1-1	Duties and responsibilities.....	1-2
Table 4-1	Terms used in this publication.....	4 -1
Table A-1	Points of contact.....	A-2
Table A-2	Registration.....	A-4
Table B-1	Points of contact.....	B-3
Table C-1	Points of contact.....	C-2
Table C-2	Reservation requirements.....	C-2
Table D-1	Points of contact	D-2
Table E-1	Points of contact.....	E-2

CHAPTER 1**GENERAL INFORMATION****101. PURPOSE**

The purpose of this ACP is to establish a secure and non-secure video-teleconferencing (VTC) capability. This capability enables the exchange of military information among the participating nations to enhance military readiness, capability and interoperability.

- a. This ACP supports the The Combined Joint Multilateral Master Military Information Exchange Memorandum of Understanding (CJM3IEM). These documents communicate all necessary interoperability standards, procedures, security instructions, and related information.

102. GENERAL

VTC provides a medium to improve the sharing of information, planning and consultation that occurs in support of multinational coalition operations. It also presents the opportunity to increase productivity by making efficient and effective use of resources allowing nations' representatives to participate in meetings without incurring travel time and costs.

103. OVERVIEW OF MULTINATIONAL VIDEOCONFERENCING SERVICES

The Multinational Videoconferencing Services described herein are available to the military communities of each participating nation. These services can be either secure or non-secure, point-to-point or multi-point.

- a. A nation's Videoconferencing Network is composed of a number of secure and non-secure videoconferencing facilities and/or one or more bridging sites.
- b. ISDN and PSTN are used to conduct point-to-point and multi-point conferences for both secure and non-secure videoconference users. Using commercial standards, the bridging site provides videoconferencing users with a wide variety of multi-point services.
- c. A secure site uses encryption equipment to encrypt information for a classified conference.

104. DUTIES AND RESPONSIBILITIES

The...	Is responsible for....
Operational Authority	<p>Ensuring that this ACP adequately describes the participating nation’s portion of the Multinational Videoconferencing Network(MVN) including: operational status, changes to the operational availability levels, resolution of user concerns with respect to the existing services and support.</p> <p>Note: The operational authority for each nation’s portion to the MVN remains with the applicable nation.</p>
CCEB EG	<p>The co-ordination of inter-nation activities will be done through the CCEB EG. The CCEB EG Chairperson will liase with other executive boards as necessary, for example with the Multinational Security Accreditation Board (MSAB).</p>
CCEB Information Security Working Group (INFOSEC WG)	<p>Advising the CCEB EG on issues related to secure Videoconferencing key material and encryption devices.</p>
Multinational Security Accreditation Board (MSAB)	<p>The accreditation of the participating nations SVTC facilities.</p>

The...	Is responsible for....
National CCEB VTC Advisors (listed at Annexes A to E)	<p>Acting as the national focal point for the SVTC program.</p> <p>Co-ordinating day-to-day management of SVTC efforts.</p> <p>Resolving SVTC issues and problems brought forth by Participants.</p> <p>Referring SVTC issues that cannot be resolved by the POCs to the appropriate authorities.</p> <p>Co-ordinate/recommend amendments to the CJM3IEM.</p> <p>Identifying the national SVTC COMSEC custodian.</p> <p>Liaison with all other national POCs on matters affecting their SVTC Facilities and/or Bridges that affect the CJM3IEM.</p> <p>Oversight of the security aspects of SVTC in accordance with the CJM3IEM</p> <p>Arranging for the submission of their national accreditation documentation to the MSAB for approval.</p> <p>Any other responsibilities required for co-ordination of SVTC.</p>
Conference Chairperson / Requestor	<p>Informing participants of all information regarding the VTC (e.g. subject, date, time in ZULU, location, duration, name of chairperson, participants & classification).</p> <p>Ensuring all participants have booked their national facilities and have the appropriate security clearances. Arranging a VTC reservation with the Videoconferencing Co-ordinator (VCC)</p> <p>Informing their local VCC of any changes to or cancellations of scheduled conferences.</p> <p>Announce at the start of a conference the security classification and/or conditions pertaining to the VTC</p>

The...	Is responsible for....
Videoconferencing Coordinator	<p>Ensuring the appropriate keymat is used for a particular SVTC (contact COMSEC Custodian for advice in necessary).</p> <p>Provide guidance with respect to the operation of the facility.</p> <p>Assisting conference chairperson with their reservation requests.</p> <p>Passing on any information regarding scheduled conferences such as cancellations of or changes to conferences.</p> <p>Be on duty one half hour before each videoconference in order to set up the equipment and for briefing chairpersons/ participants on the use of the equipment.</p>
Bridge Operator	<p>Reserving all requested national bridge sites for the requested dates/times. Notifying the chairperson/requester when national bridges have been booked and confirmed.</p> <p>Ensuring the appropriate keymat is used for a particular SVTC.</p>
National Participant	<p>Booking their local site</p> <p>Secure VTC - arranging for the connection to their national bridge and ensuring the bridge has been informed of SVTC</p> <p>Non-Secure VTC – to provide VCC with phone number for host nations bridge.</p>

Table 1-1 Duties and responsibilities

1. Canada will be responsible for the production, administration and dissemination of all cryptographic keymat in support of the SVTC through normal COMSEC channels. Each Nation will be responsible for internal distribution of the keymat.

Note: Information exchanged by a SVTC utilizing CCEB keying material shall be releasable to all member nations regardless of whether they are participating in that SVTC or not. CCEB keying material shall not be used if it is any participating nation's intention to preclude releasability to another CCEB member nation.

2. It is the responsibility of each individual nation to provide VTC facilities to meet the CCEB requirement.

3. Each participating nation is responsible for producing SOPs for their bridge.
4. Each participating nation will bear the full cost it incurs in making, managing and administering any CCEB VTC capabilities.

105. CONCEPT OF OPERATIONS FOR VIDEOCONFERENCING NETWORK SERVICES

a. Alternate Bridge Sites:

It is anticipated that as nations VTC bridges become operational they will be declared to the CCEB as an alternate bridge site to host multinational VTCs, subject to availability

b. Web Sites:

Nations are encouraged to create a web site. This would increase the accessibility to the information. Once the web site is created, it should include links to the other nations' videoconferencing web sites and likewise, the international working groups will include links to the site from their websites.

c. System Overview:

- (1) The Multinational Videoconferencing Network is composed of the portions of each participating nations' VTC networks that have been made available to allow the participating nations to conduct non-secure and secure (up to secret releasable to AUSCANNZUKUS) Videoconferences.
- (2) The Multinational Videoconferencing Network allows face-to-face non-secure or secure conferences to take place between the military communities of the participating nations.
- (3) Bridging facilities available to the participating nations are listed in the country Annexes A-E. These bridging facilities have secure and non-secure capabilities and support point to point and/or multi-point videoconferencing.

d. Levels of support:

The level of support is subject to the availability of facilities at the time of the conference and operational requirements. Details of the normal hours of operation of each participating nation's facilities are shown in Annexes

A to E.

- e. Future requirements:

Taking cognisance of evolving VTC technology participating nations shall endeavour to ensure that interoperability between nations is maintained. Such issues, to name a few, include changes in system architecture (i.e., IP based system) and cryptographic equipment, etc.

- f. New users:

New users wishing to access the CCEB VTC network are to consult their national POC (see Annexes A to E) who will advise of registration requirements.

106. LIAISON

Direct liaison between nations subject matter experts for day-to-day operations is authorized. Changes or proposals to amend policy or network procedures must be staffed through the appropriate national channels.

107. ACCESS TO FACILITIES

- a. Each Participant may permit use of its facilities by personnel of another Participant, provided the visiting personnel have appropriate security clearances.
- b. Requests for use by personnel of one Participant to facilities of the other Participant will be coordinated through official channels and will conform to the established visit procedures of the host country.

CHAPTER 2**INTEROPERABILITY REQUIREMENTS****201. GENERAL**

- a. Nations are to ensure interoperability between each participating nation's VTC services is maintained, maximizing the effectiveness and availability of both secure and non-secure services.
- b. Commonality in cryptographic equipment, H.320 commercial standard, and the capability to operate at 128 Kbps are the minimum requirements for the CCEB VTC network. Operation at 56/64 Kbps will be accepted for deployable devices.
- c. Some nation's videoconferencing services allow for the use of advanced capabilities such as document sharing/collaboration it should be noted that a site participating in the conference might not support these capabilities.
- d. Advancements in technology will provide the opportunity to enhance the network. Nations should be mindful that changes to national facilities could be detrimental to the interoperability of the network. As such, changes that may affect interoperability should be brought to the attention of the CCEB through the national POC.

CHAPTER 3

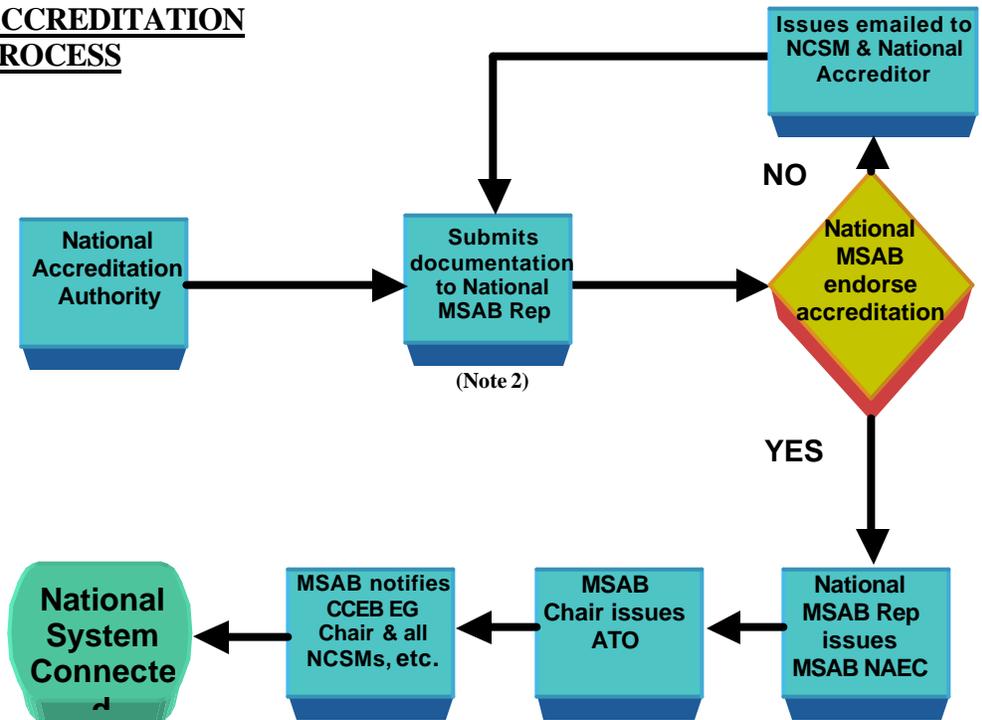
SECURE VIDEOCONFERENCING SERVICES

301. GENERAL

- a. All participating bridge sites and VTC facilities need to be certified and accredited before conducting a secure VTC. Each nation is responsible for the accreditation of facilities within their nation through their MSAB representative.
- b. The CJM3IEM captures the rules and procedures under which the CCEB nations agree to conduct SVTCs.
- c. The CJM3IEM permits the exchange of Military Information at SECRET (releasable to AUSCANZUKUS) among the participating nations using SVTC.

302. MSAB PROCEDURES

a. **ACCREDITATION PROCESS**



3-1

ORIGINAL

System Accreditation Notes:

1. Before a national system connection is proposed and the security and accreditation process implemented, CCEB Executive Group (EG) approval must be sought. The CCEB EG will notify the Multinational Security Accreditation Board (MSAB) of pending connection.
2. The National Accreditation Authority (NAA) of each nation certifies to their national MSAB representative that their facilities have been accredited to process and protect information up to and including SECRET releasable to AUSCANZUKUS.
3. The national MSAB Representative issues the MSAB National Accreditation Endorsement Certificate (NAEC) notifying the MSAB chair that their NAA has approved the accreditation of their national facility. The MSAB chair issues an OPCWAN ATO to the NCSM and the Chairs of the CCEB EG, CWAN SWG and MSAB.

303. KEY MATERIAL MANAGEMENT PROCEDURES

- a. COMSEC Accounts. Each communication entity that operates a CCEB Multinational Videoconferencing Service (MVS) must be supported by national COMSEC account in order to be issued the appropriate network key. Each request to establish a new CCEB MVS must identify its support COMSEC account and supporting National Distribution Authority (NDA).
- b. Classification. All of the CCEB MVS are capable of VTC activity at an UNCLASSIFIED level. When authorized to do so, an appropriately classified key is distributed and implemented, individual CCEB MVS sites may transmit information at the SECRET level.
- c. Controlling Authority (CA) Responsibilities. With respect to the management of the CCEB MVS keymat, the Canadian Forces Crypto Support Unit (CFCSU), Key Management Authority (KMA) is responsible for:
 - (1) The issue of the required CCEB MVS keymat;
 - (2) Keep holders apprised of its effective status;
 - (3) Direct the implementation of temporary crypto period extensions;and

- (4) Receive and evaluate reports of COMSEC incidents affecting the CCEB MVS keymat and direct actions, such as unscheduled supersessions, to reduce the security impact of reported compromises.

- d. Key Usage. CCEB MVS keymat may only be used for VTC between member nations. Use of the CCEB MVS keymat is NOT AUTHORIZED for any other purpose.

- e. Key Distribution. CFCSU will produce and issue the CCEB MVS keymat to each country's NDA. The NDA will then be responsible to distribute the keymat to their CCEB MVS sites using their own courier services. When CFCSU selects a date for the first edition to become effective, automatic re-supply will be effected. NDAs will be notified of the keymat status so that correct status information may be inserted in their respective COMSEC status documents and databases. Individual NDAs are responsible for ensuring that COMSEC regulations regarding accounting, handling and destruction procedures are maintained.

- h. Crypto period Extensions. To meet urgent operational requirements, the Canadian National System Management Centre (NSMC) may extend the crypto period by 2 hours. Longer extensions require prior authorization from CFCSU/DNDKMA. On occasions where a VTC will bridge over to a new day (all times Zulu), crypto change must be performed immediately following the termination of the VTC but at no time shall the extension exceed 2 hours. Segments must be destroyed within 12 hours of being superseded.

- i. Safeguarding Keyed KIV-7HSs. When its associated crypto ignition key (CIK) is extracted from the KIV-7HS with which it is associated and is either securely stored or removed from the terminal area, partially keyed KIV-7HSs become UNCLASSIFIED, controlled cryptographic items (CCIs) and may be left in unmanned dial-up subscriber terminal spaces provided the door is locked and its key is controlled. Extracted CIKs also become UNCLASSIFIED but the finding of an unsecured CIK in an unmanned area is a reportable COMSEC incident.

304. REPORTING LOSS OR COMPROMISE OF KEY MATERIAL

- a. Report loss/compromise to Controlling Authority identified in paragraph 303 of this document through the appropriate National COMSEC Authority. Reportable KIV-7HS Incidents include:
 - (1) Retaining effective or superseded Transmitted Electronic Key (TEK). Unauthorized retention of exposed segments of effective or superseded TEK;
 - (2) Unauthorized crypto period. Using a KIV-7HS TEK beyond its authorized (or properly extended) crypto period;
 - (3) Mishandling of KIV-7HS CIK. Finding an operational CIK in an unmanned CCEB MVS area;
 - (4) Exposed TEK segments. Failure to properly store exposed TEK segments when not in use; and
 - (5) TEK/Short-title/Effective date Association. In unsecured communications, associating a CCEB MVS key short-title and edition identifier with its effective period.

305. SECURITY PROCEDURES

- a. All Classified Information and Data exchanged under the CJM3IEM will be stored, handled, transmitted, and safeguarded in accordance with national security laws and regulations and the bilateral General Security Agreements/Arrangements that already exist between the Participants.
- b. Classified Military Information and Data will be transmitted only through official government-to-government channels or through channels accredited by the Designated Security Authorities of the Participants. Such Classified Information and Data will bear the levels of classification, denote the country of origin, and the conditions of release.
- c. Each Participant will take all lawful steps available to it to ensure that Classified Information and Data received under the CJM3IEM is protected from further disclosure unless the originating Participant consents to such disclosure. Accordingly, each Participant will ensure that:
 - (1) It will not release any Classified Military Information and Data

received under this MOU to any other government or national organization, or other entity of a Third Party without the prior written consent of the originating Participant in accordance with the procedures described in CJM3IEM.

- (2) It will not use any Classified Military Information and Data received under the CJM3IEM for other than the purpose provided for in this MOU.
 - (3) It will comply with any distribution and access restrictions on Classified Military Information and Data that is provided under the CJM3IEM
- d. Each Participant will maintain the security classification assigned to Classified Information and Data by the originating Participant and will afford to such Classified Information and Data at least the same degree of security protection provided by the originating Participant.
 - e. The Participants will investigate all cases in which it is known or where there are grounds for suspecting that Classified Information and Data received under the CJM3IEM has been lost or disclosed to unauthorized persons. Each Participant will also promptly and fully inform the other Participants of the details of any such occurrences, and the final results of the investigation and of the corrective action taken to preclude recurrences.
 - f. Each Participant will ensure that access to Classified Information and Data provided for under the CJM3IEM is limited to those persons who possess requisite security clearances and have a specific need-to-know.
 - g. The existence and content of the CJM3IEM are UNCLASSIFIED. Information up to and including SECRET may be exchanged using the CCEB Secure VTC

306. EXCHANGE AND USE OF INFORMATION

- a. In accordance with the CJM3IEM

307. CONTROLLED UNCLASSIFIED INFORMATION

- a. In accordance with the CJM3IEM

CHAPTER 4**GLOSSARY OF TERMS****401. TERMS USED IN THIS PUBLICATION**

Term	Agreed Meaning
AAD	Access Approval Document
ACP	Allied Communication Publication
AUSCANNZUKUS	Australia Canada New Zealand United Kingdom United States
Bridge	Capability to host Multi-Nation SVTCs (usually requires a multi-point control unit (MCU))
CA	Controlling Authority
CCEB	Combined Communications-Electronics Board
CCEB EG	Combined Communications-Electronics Board Executive Group
CCI	Controlled Cryptographic item
CFCSU	Canadian Forces Crypto Support Unit
CFNOC	Canadian Forces Network Operations Centre
CIF	Common Intermediate Format
CIK	Crypto Ignition Key
CJM3IEM	The Combined Joint Multilateral Master Military Information Exchange Memorandum of Understanding
CODEC	Coder/decoder
COMSEC	Communications Security
CRCS	Conference Reservation and Control System
CWAN	Coalition Wide Area Network
DAA	Designated Approval Authority
DCCS	Digital Access and Cross-Connect Systems
DCMC	Defence Crisis Management Centre
DISN	Defense Information Systems Network
DND	Department of Defence
DSVE	Defence Secure Videoconferencing Environment
DTG	Date Time Group
DVS	Defense Video Services
DVCN	Defence Video Conference Network - Secure
Facilities	Secure Video Teleconferencing studios
FTR	Federal Telecommunications Recommendation
H.320	International VTC standard for PSTN/ISDN
IATO	Interim Approval to Operate
INFOSEC	Information Security
IP	Internet Protocol

Term	Agreed Meaning
ISDN	Integrated Services Digital Network
Kbps	Kilobits per second (1000 bits per second)
Keymat	Keying Material
KIV	Cryptographic device
KMA	Key Management Authority
MIC	Multinational Interoperability Council
MOU	Memorandum of Understanding
MSAB	Multi-National Security Accreditation Board
Multinational Videoconferencing Services (MVS)	The Multinational Videoconferencing Services is a virtual combination of the portion of each participating nation's Videoconferencing Network that has been made available to the international defence (strategic and operational) communities.
Multi-point conference	A multi-point conference is a connection of three or more videoconferencing sites. Multi-point conferences are a little more complex and require additional equipment. The additional equipment is called a Multi-point Control Unit (MCU). (Is their a maximum number of participants you can have in a Multi-point Conference)
Multi-point Control Unit (MCU)	An MCU allows all of the conference participants to see and hear each other. All sites are connected to a Multipoint Control Unit (MCU, or "Bridge").
NAA	National Accreditation Authority
NAEC	National Accreditation Endorsement Certificate
NCSM	National Connection Security Manager
NDA	National Distribution Authority
NSA	National Security Agency
Operational Authority	Oversees that requirements are met prior to allow connection to the network.
POC	Point of Contact
Point-to-point conference	A point-to-point conference is a single videoconference facility connected to another videoconferencing facility by a transmission path. Two sites connect together by one site dialling the other site. The two sites can see and hear each other.
PSTN	Public Switched Telephone Network
QCIF	Quarter Common Intermediate Format
RAAF	Royal Australian Airforce
Secret	Classified up to and including SECRET releasable to Australia, Canada, New Zealand, United Kingdom, and United States (AUSCANNZUKUS).

Term	Agreed Meaning
SOPs	Standard Operating Procedures
SVTC	Secure Video Teleconferencing
TEK	Transmitted Electronic Key
UCC	Universal Conference Control
UVCN	Unclassified Video Conference Network
VAS	Voice-Activated Switching
VCC	Video Conferencing Co-ordinator
VCN	Videoconferencing Network
Videoconferencing	Videoconferencing is the means by which two or more locations (containing videoconference equipment) are linked electronically allowing the participants in one location to see and hear the participants in the other location-(s). Technical types define videoconferencing as "an exchange of digitised video images and sounds between conference participants". This digitised exchange is made possible by CODECs, which are coder/decoders. They take analogy input (the video and sound) and convert it to digital information for transmission.
VNOC	Video Network Operations Centre
VOC	Video Operations Centre
VTC	Video Teleconferencing
WG	Working Group
ZULU	Time Zone

Table 4-1 Terms used in this publication

ANNEX A

AUSTRALIAN DEFENCE VIDEOCONFERENCING NETWORK**1. National Overview**

The Australian Defence Secure Videoconferencing Environment (DSVE) has been designed to provide a VTC capability, up and including the SECRET releasable to Australia, Canada, New Zealand, United Kingdom and the United States, to approved Australian Defence units. The Video Network Operations Centre (VNOC), or Bridge, is located in RAAF Glenbrook New South Wales. Contact details are detailed at Appendix 1. The Australian Department of Defence do not have a contract for unclassified VTCs, however requests for multi-point non-secure VTCs can be booked through the VNOC if required. Unless approved separately, multi-point unclassified VTCs will be billed to the requesting unit or command.

The operation of the DSVE capability is the responsibility of support contractors. The Commonwealth is responsible for operating individual video conferencing end points. All secure conferences are initiated manually from the VNOC. Unless advised otherwise all ISDN calls from the VNOC shall be at 128kb bonded.

2. Security General

All SVTCs are cryptographically protected utilising approved Government Furbished Cryptographic Equipment. DSVE policy requires that the transmission of all SVTCs, be performed through the VNOC.

The VNOC utilises various keying material for specific SVTC, i.e. national, bi-lateral and multi-lateral, information. It is essential to include all participants when booking with the VNOC. (see paragraph 106). For example if a SVTC is to be conducted in support of CCEB activities the VNOC shall utilise specific CCEB keymat vice alternate keymat. As stated in Chapter 1, information exchanged by a SVTC utilising CCEB keying material shall be releasable to all member nations regardless of whether they are participating in that SVTC or not. CCEB keying material shall not be used if it is any participating nation's intention to preclude releasability to another CCEB member nation.

The Defence Signals Directorate is the National COMSEC Custodian for International Cryptographic Keymat. The re-keying of local cryptographic equipment in support of SVTC remains the responsibility of local area commands and units. Local Security Orders and appropriate staff should be consulted, in the first instance, to offer guidance on the operation of cryptographic equipment and keymat for SVTC. In the absence of this support advice may be sought from the VNOC.

3. Hardware/Software/Firmware

The VNOC has one Multi-point Control Unit (MCU) assigned for use for Coalition SVTC, i.e. bi-lateral, multi-lateral (CCEB and/or MIC), and one for National SVTC. Although a separate MCU has been assigned for coalition SVTCs, national operational requirements shall take precedence.

4. National Booking requirements

Requests to establish a SVTC should be directed to the VNOC Supervisors on the contact numbers and/or e-mail addresses detailed at Appendix 1. Note: As previously stated the Australian Department of Defence does not have a contract for unclassified VTC however the VNOC Supervisors will accept and co-ordinate requests from Defence customers. Unless approved separately, unclassified VTC will be billed to the requesting unit or command.

Guidelines for establishing a VTC are detailed in paragraph 6 Registration. . Note that there are additional requirements for Secure VTC.

5. Points of Contact

Responsibility	Appointment	Contact Information	Remarks
CCEB VTC National Advisor	Executive Officer Regional Relations Office of the Chief Information Officer ADHQ	EO RR R1-3-A134 Russell Offices CANBERRA ACT 2600 AUSTRALIA PH: 61-2-6265 7027 FAX: 61-2-6265 6106	POC for multinational SVTC inquiries Message Address: ADHQ (Insert quote ADHQ for Executive Officer Regional Interoperability R1-3- A134 unquote in first lines of text)
Defence Video Conferencing Manager	Defence Video Conferencing Manager Defence Communications Centre	Defence Video Conferencing Manager Defence Communications Centre 25 Napier Close Deakin ACT 2600 Ph +61 2 6265 8804 Fax +61 2 6269 4130	Primary point of contact for Australian National secure video conferencing policy inquiries

VNOC (Bridge) Co-ordinator	VNOC Supervisor Ausvidcon@defence.gov.au	DSVE Building 139 RAAF Glenbrook GLENBROOK NSW Australia Ph: 61-2-4737 7667 Fax: 61-2-4737 7866 e-mail: Ausvidcon@defence.gov.au	Primary point of contact for Secure VTC 'operations' Bridge hours of operation: (ZULU) Mon/Wed/Thu/Fri 2100 hrs – 0700 hrs Zulu Tue 2030 hrs – 0700 hrs Zulu
National COMSEC Custodian	Information Security Group Cryptographic Liaison Officer	Defence Signals Directorate Locked Bag 5076 KINGSTON ACT 2605 Australia Ph: 61-2-6266 5762 Fax: 61-2-6265 0328	Message Address: quote DSD CANBERRA unquote DSD is the National COMSEC Custodian. Local cryptographic re-keys remains the responsibility of local units or commands.

Table A-1 Points of Contact

6. Registration

Guidelines for establishing a VTC

Action Officer	Requirements	Remarks
Step 1: Requesting Officer	Provide the videoconference co-ordinator (VCC) with the following information: <ol style="list-style-type: none"> 1. requested time and location including total number point to point or multi-station call 2. site/s points of contact 3. security level of VTC (up to SECRET – see remarks opposite) 4. are any audio-visual peripherals required e.g. PowerPoint 5. Contact details of requesting officer 	<ol style="list-style-type: none"> 1. Normally this person will also be the VTC Chairperson 2. The Requesting Officer should ascertain whether the Secure VTC is in support of CCEB/MIC activities or otherwise and that all participants hold required security clearance 3. For non-secure multi-point VTC the Requesting Officer will need to provide additional details for billing purposes
Step 2: VCC	The VCC shall: <ol style="list-style-type: none"> 1. Book local site 2. Confirm distant site/s through appropriate POC/VCC 3. Confirm classification of VTC – secure or non-secure 4. If secure, confirm SVTC is in support of CCEB or otherwise 5. Contact the appropriate agency for final booking and provide, as a minimum: <ul style="list-style-type: none"> Request Requested dates/times (ZULU) for the conference Request Alternate dates/times if primary time not available Advise Requesting Officer of VTC booking	<ol style="list-style-type: none"> 1. Bridge staff will normally contact each nominated site POC and confirm details provided 2. Normally Requesting Officer will also be the VTC Chairperson For SVTCs the VCC should ensure, at least 48 hours before commencement of the VTC, correct cryptographic keymat is in place at the local site.

Table A-2 Registration

APPENDIX 1

HOW TO CONDUCT A SUCCESSFUL VTC

1. Introduction

- a. Video Teleconferencing is a very effective method to collaborate and share information with colleagues at geographically dispersed sites. To ensure that VTCs are effective and run smoothly, the following generally accepted guides to behaviour and technique have been developed.

2. Testing

- a. Prior to the VTC going 'live', the VTC site manager should have tested and adjusted the audio and video to provide optimal performance. The camera should be 'zoomed' to the key speaker(s), with pre-adjusted settings allowing panning to other participants. If the camera can not pan than participants should be in one shot.
- b. Assuming the audio and video levels are acceptable, participants in the VTC should resist the temptation to make further adjustments, including moving the microphone, during the VTC. However, if the audio and/or video deteriorate to a less-than-acceptable level, the affected site should advise the Chairman and seek resolution of the problem.
- c. At the beginning of the conference and at any time during the conference, the Chairman should make sure that all the participating sites can see and hear your site. Don't hesitate to ask other participants to speak up if necessary.

3. Audio and Video

- a. Speak clearly and act naturally during a VTC. If the main language is not the normal language for some participants, extra care should be taken to ensure that they understand the issues and are included in discussion. Use verbal and visual cues as appropriate.
- b. A good quality speakerphone should be available as a backup for use as an audio teleconference in case there are problems with the video. Participation using audio only is preferable to not participating at all.
- c. There is often a transmission delay of up to one second. A speaker should pause when expecting or requesting comment from far-end participants, and let the far-end speaker finish before starting to talk.
- d. On multipoint VTC, the local microphone should be muted when not in use or when another site is speaking. De-mute the local microphone to talk.

UNCLASSIFIED
DRAFT APPENDIX 1 TO ANNEX A TO ACP 220

- e. Extraneous noises (rustling papers, moving chairs, noisy air conditioners etc) and side conversations that might normally go unnoticed in a face to face conference can create technical problems in a VTC and distract from the prime conversation. In multipoint VTC, the video display will automatically select the site generating noise, whether intentional or not.

4. Dress

- a. Selection of attire for VTC meetings is naturally the prerogative of participants. However, experience has shown that ‘solid colour’ medium blue and pastel colours coupled with dark outer wear (suit coat etc) project well. Striped, checked, plaid or white clothing can often cause a strobbing or ‘venetian blind’ effect.

5. Presentations

- a. When creating presentation materials such as agendas, charts etc. use large fonts to compensate for low screen resolution. Fonts smaller than 14pt. Courier can be difficult to see. Use graphics that are easy to see and understand.
- b. Where possible, distribute presentation material to each site prior to the VTC. This allows for poor display resolution during the live presentation, and for the possibility that presentation material may not be displayed due to technical or operator problems.
- c. Provide adequate time for participants at remote sites to read and/or understand visual aids/presentations.
- d. Avoid moving presentation materials around. The far-end screens can take some time to update. If necessary, use a pen or pencil as a pointer and leave it in one spot while you make your point. This works better than using your finger, which one tends to move around and which can cause the document or transparency to move around.
- e. If a site other than yours is making a presentation, mute the local microphone. This will prevent needless image switching caused by background noises in your room.

6. Moderator/Facilitator/Chairman Roles and Responsibilities

- a. Distribute Agenda and presentation material (electronically, by fax or other suitable means) in sufficient time before the meeting to allow all participants to be familiar with the program and material to be presented.

UNCLASSIFIED
DRAFT APPENDIX 1 TO ANNEX A TO ACP 220

- b. Prepare adequately for the meeting. The Chairman is a key player to ensure that the VTC is successful and effective.
- c. Start and conclude the meeting on time. VTC facilities are often heavily booked and extension to on-air time may not be possible.
- d. Always conduct a roll call/poll all sites for video and audio, at start and periodically during conference. If some meeting participants have not met previously, invite them to introduce themselves
- e. It is often useful to poll sites in a predetermined sequence. This ensures that all participants know when they should expect to be included, and ensures that no sites are excluded when opinions or input is being sought.
- f. Introduce key participants at local site and invite each site leader to introduce participants.
- g. Highlight expected objectives/goals and desired outcomes from VTC meeting.
- h. During the VTC, direct questions to specific person/site to prevent multiple responses.
- i. A key role of the Chairman is to manage and control the conduct of the meeting. If one (or more) party(s) is dominating the discussion, the Chairman should intercede and seek input from other participants.
- j. If the VTC includes open discussion between three or more locations (open discussion is not recommended at more than three sites), the Chairman should maintain control and intercede when two or more locations attempt to speak at the same time.
- k. Summarise key points and plan /agree follow up actions. Allow a short but adequate period prior to the scheduled conclusion time for the summary.
- l. Be aware of fatigue among participants. Schedule 10 minute breaks each hour if the VTC if planned to be longer than one hour.

ANNEX B

CANADIAN VIDEOCONFERENCING NETWORK**1. National Overview**

In Canada, the Department of Defence (DND) provides secure and non-secure standards-based point-to-point and multi-point videoconferencing services to major DND installations across Canada and abroad. To this end, DND has installed two Avaya Multi-point Conferencing Units (MCU) and associated equipment. These MCUs allow videoconferencing end-points to participate in video, audio and data conferencing. One MCU is for non-secure conferencing and the other is for secure conferencing.

DND's Videoconferencing Network is composed of the Unclassified Videoconferencing Network (UVCN) and the Defence Videoconferencing Network (DVCN). The DVCN is used for secure conferencing requirements and the UVCN is used for non-secure requirements.

2. Hardware/Software/Firmware

DND's unclassified and secure MCUs permit DND to choose the speed and number of locations on a call. The unclassified and secure MCUs have the following control modes:

- a. Voice-Activated Switching (VAS) — The MCU automatically switches the video display when the speaker changes.
- b. Presentation Mode — Suitable for training sessions or presentations, participants see the speaker at all times, while the speaker sees the questioner.
- c. Broadcast and VAS with Auto Scan — Participants see the speaker at all times, and the speaker see participants in each location on a timed, predetermined, rotating basis.
- d. Universal Conference Control (UCC) allows users to control their videoconference with a touch-tone phone. UCC can be used to change conference modes, browse, change conference broadcaster, and drop selected endpoints from a conference, roll call and terminate a conference. Note: This feature is only available on the unclassified MCU.

The unclassified and secure MCUs are managed via a Conference Reservation and Control System (CRCS). CRCS is a Microsoft® Windows NT® or Windows® 2000-based automated system for reserving and controlling conferences, conference rooms, and video networking resources.

The unclassified and secured MCUs provide the following video processing capabilities:

a. Continuous Presence Plus:

Connect up to 25 locations with Continuous Presence Plus in a single conference via both video and audio. This feature allows one or more participants to see up to four sites in the conference at one time. Each Continuous Presence Plus conference shows this “quad-image” from the start of the conference. Any of the quadrants can be fixed or “locked in” on a particular location or they can proceed with VAS. This allows you to have an executive location speaking and have their image switched into a quadrant.

b. Speed Matching:

Speed Matching makes it easier to bring desktop and group users into a single conference by allowing video endpoint operating at different speeds to join a conference, without all sites having to drop to a lower speed to accommodate every video endpoint.

c. H.320 Translator:

The H.320 translator allows H.263 endpoints to maintain their improved quality while communicating with endpoints using the H.261 standard. Conferences using the H.320 translator are supported in the full screen mode, while conferences while using the H.263 exclusively are supported in both the full screen and Continuous Presence Plus mode.

The unclassified and secure MCUs provide H.320 multipoint data conferencing using the T.120 standard.

The unclassified MCU is capable of mixed conferences consisting of endpoints using circuit-switched (H.320) and Internet Protocol (IP)-based (H. 323).

The unclassified and secure MCUs both support a variety of networking interfaces, including T1/E1, PRI, BRI trunk-side and line-side, 10/100BaseT, V.35/RS449/RS366, and DCP.

3. Contacts

Responsibility	Appointment	Contact Information	Remarks
CCEB National POC	Dave Crittenden Major Directorate Information Management Strategic Planning (DIMSP) Interoperability Coordination 4-4	Tel: (613) 995-9451 Fax: (613) 992-4223 Secure Fax: (613) 996-6828 or (613) 992-6029 Attention: DIMSP 4-4 Email: Crittenden.DH@forces.ca	
Bridge (MCU) Operations	Canadian Forces Network Operations Centre	Tel: (613) 991-2549 Email: videocoferencing@forces.gc.ca	
National COMSEC Custodian	Mr. J.G. Trottier Canadian Forces Crypto Support Unit	Tel: (613)-945-7504 Email: Trottier.JG@ADM(IM)CFCSU@Ottawa-Hull	
Engineering Support	Robert Streeter Captain Directorate Telecommunications Spectrum and Engineering Support (DTSES 2-5-3)	Tel: (613) 990-5237 Fax: (613) 998-6277 Email: streeter.rs@forces.gc.ca	

Table B-1 Points of contact

4. National Reservation Requirements

Canadian Forces Network Operations Centre (CFNOC) is the central scheduling agency for all secure and non-secure CCEB multi-point and point-to-point videoconferences. The normal hours of operation are Monday through Friday 1200Z to 2400Z. The following shall be the procedures followed for multi-point and point-to-point reservations:

- a. The person requesting the conference (the requester) must complete a "Reserve a Multi-point videoconferencing" form found at DND's Videoconferencing Intranet web site <http://vc.mil.ca>. and send to the CFNOC MCU Bridge Operator, by clicking the SUBMIT button at the bottom of the form. If this service is not available contact the CFNOC MCU Videoconference bridge operator with the following information:
 - (1) Requested dates and times for the conference, including alternative dates and times in case the requested date/time is not available;
 - (2) Type of conference (secure or non-secure);
 - (3) Title of conference;
 - (4) Sites required for conference; and
 - (5) At least one representative participant/contact person at each site; and requester's contact information.
- b. The requestor must ensure that their site is available and reserved for the conference.
- c. CFNOC bridging staff shall attempt to reserve all requested sites for the requested dates/times using the reservation procedure agreed upon individually with each site.
- d. CFNOC bridging staff shall notify all sites when sites have been confirmed and reserved. Each site is then responsible for notifying those in the area that are to attend.

Prioritization: Requests for conferences will be scheduled on first come first served basis. When making a reservation, there should be a high level of confidence that, once scheduled, a conference will go ahead as planned. To maintain the integrity of the system, once a reservation has been confirmed it should, in general, be considered final.

In the event that National users and CCEB users simultaneously wish to reserve a videoconferencing site, it will be up to the CFNOC staff to coordinate between the two groups. If CFNOC bridging staff are unable to have the sites voluntarily reschedule their videoconference, then priority will be given to National requirements and then CCEB requirements.

5. Registration

The following information is required to register with the Canadian Bridging service:

User Profile:

Site Name:

Video Conference Co-ordinator:

Name:

Position:

Contact information during working hours:

Telephone #:

Mobile (Cellular phone #):

Facsimile #:

Internet Email Address:

Contact information after working hours:

Telephone #:

Mobile (Cellular phone #):

Facsimile #:

Internet Email Address:

Technical Support Contact:

Telephone #:

Mobile (Cellular phone #):

Facsimile #:

Internet Email Address:

Contact information after working hours:

Telephone #:

Mobile (Cellular phone #):

Facsimile #:

Internet Email Address:

Room Profile:

Room Address:
Room/Floor No:
City:
Province/State:
Country:
Postal Code/Zip:

Room Phone Number:

Room Capacity: _____

Room Features: _____ VCR _____ White Board _____ Document Camera
_____ PC Interface _____ Graphics Monitor _____ Auxiliary Camera.

Other Features:

Equipment Profile:

CODEC Manufacturer:

Model:

Software Revision:

System Type: _____ Desktop _____ Dialup _____ LAN _____ Dedicated

Protocol: _____ H.320 _____ H.323

Video Mode: _____ H.261 _____ H.263 _____ H.CTX+ _____ MRV _____ SG4

Audio Mode: _____ G.711 _____ G.722 _____ G.728

Data Mode: _____ T.120 _____ Other

Network Profile: Local Carrier Name:

Access Service: _____ SW56 _____ ISDN BRI _____ ISDN PRI _____ T1

Type: _____ MEGA Stream _____ Satellite

ANNEX C

NEW ZEALAND DEFENCE FORCE VIDEOCONFERENCING NETWORK

1. National Network Overview

The New Zealand Defence Force currently operates a multipoint bridge capable of supporting up to 4 locations in both the non-secure and secure mode. Each location can be supported up to 128kb/s and variable speeds up to this rate can be accommodated. In addition there are a number of locations throughout the country capable of operating point to point in the non-secure and secure modes although some locations are only capable of non-secure operation. The NZ VCC can advise on these locations.

2. Hardware/Software/Firmware

The bridge is a 4-port PictureTel Prism model. The VTC terminals vary between locations but are primarily PictureTel Concorde 4000 series in the main headquarters.

3. Points of Contact

Responsibility	Appointment	Contact Information	Remarks
National POC	Staff Officer Engineering (SO Eng) Directorate of Joint Command, Control Communications, and Information Systems (DJCIS) HQ New Zealand Defence Force	Tel: +64 4 496-0162 Fax: +64 4 496-0159 Email: john.rosevear@nzdf.mil.nz	
Bridge Co-coordinator (Primary contact for VTC services)	Video Conferencing Bridge Operator Defence Communications Unit (DCU)	Tel: +64 4 496-0174 or +64 4 496-0220 Fax: +64 4 496-0269 or +64 4 496-0229 Internet email: videoconferencing@nzdf.mil.nz	

Responsibility	Appointment	Contact Information	Remarks
Video Teleconferencing Co-coordinator (VCC)	SVTC Operator Defence Communications Unit (DCU)	Tel: +64 4 496-0174 or +64 4 496-0220 Fax: +64 4 496-0269 or +64 4 496-0229 Internet email: videoconferencing@nzdf.mil.nz	
Technical Contact	Staff Officer Engineering (SO Eng) Directorate of Joint Command, Control Communications, and Information Systems (DJCIS) HQ New Zealand Defence Force	Tel: +64 4 496-0162 Fax: +64 4 496-0159 Email: john.rosevear@nzdf.mil.nz	

Table C-1 Points of contact

4. National Reservation requirements

The normal hours of operation are 2000 to 0430 Zulu Monday to Friday. Any users required to arrange a CCEB videoconference should:

Step	Task	Responsibility
1	Ensure all participants are available for the conference and reserve the conference room	Conference Chairperson
2	Contact their local VTC operator to reserve the equipment advising the participants, time, place, and classification required for the conference	Conference Chairperson
3	Seek assistance on how to facilitate a CCEB videoconference from either the VCC	Local VTC Operator
4	Either: <ul style="list-style-type: none"> a. Reserve the far end facility if conference is to be a point-to-point conference. or b. Contact the CCEB Bridge facility operator to request a multipoint conference. 	Local VTC Operator or VCC as appropriate

Table C-2 Reservation requirements

5. Registration

There are no formal registration procedures. Contact should be made with the VCC who will arrange for link testing prior to the conference if the link has not been used previously.

6. Scheduling Priority

They are based on a first come first served basis although operational requirements at the requested time will determine the priority given to a particular conference.

ANNEX D

UNITED KINGDOM'S VIDEOCONFERENCING NETWORK

1. National Overview

The United Kingdom's Videoconferencing Network (UKVCN) has its main control point at the Defence Crisis Management Centre (DCMC), located within the MOD in London. This facility deals almost exclusively with secure Videoconferencing, but does have the capability to participate in non-secure conferences.

The DCMC uses point-to-point links, but is currently developing an Accord MGC 100 MCU, which will work alongside the analogue Bridge. Connections are made to the Canadian or the US secure or insecure bridges for conferences that would include Australia, New Zealand, Canada, the United States and the United Kingdom. Regular Videoconferencing takes place between the UK and the US or Canada. There is no direct connection to either Australia or New Zealand, although they are both technically possible.

The UKVCN uses ISDN links, both of a dial-up and permanently connected nature. These links vary from low speed connections to links that are almost of television quality.

2. Hardware/Software/Firmware

The analogue Bridge, which is predominantly used, has the capacity for up to 9 participants in a single conference. Imagecom CD400 Codecs are the backbone of the network. They are multi-tasking Codecs that can be used from 64k to 2Megabits at G704, RS530 or X21, depending on the distant end equipment type. All participants are connected independently and are 'multiplexed' using various audio and video matrices.

The MCU, is an Accord MGC100 and has only been used for low speed X21 link conferencing. This Bridge has provided a "future proof" capability for the DCMC. A variety of investigations and tests are currently taking place to enable this Bridge to be used for RS530, ISDN and IP.

3. Contacts

Responsibility	Appointment	Contact Information	Remarks
National VTC Coord	J6 Pol SO2	Tel: +44 207 218 6016	Cord for CCEB & MIC VTC
National POC	DCMC Coord Cell	Tel: +44 207 218848/56/57	First point of contact for permission to use system.
Bookings/Permission	CSDSO Cell 24/7 Manning	Tel: +44 207 2188851	Contact should ONLY be made once permission has been granted.
Videoconferencing	Videoconferencing Services	Tel: +44 207 2188815	For day-to-day running of UKVCN
Technical Contact	Videoconferencing Technical Specialist	Tel: +44 207 2188798	For testing of new links/advice

Table D-1 Points of contact

4. Reservation Requirements

The facility described above is for the exclusive use of the Defence Crisis Management Organisation and permission for external agencies to use the facility is given only by prior agreement with AD DCMC. Should a location wish to use these facilities the first point of contact should be the DCMC Coord Cell - number is given in the table above.

If permission is granted by the DCMC Coord Cell, the following procedure should be adopted to book a conference:

- a. The person requesting a conference must contact the Bookings office to submit the requirements. The staff will need to know the following information:
 - (1) Preferred date and time;
 - (2) Title of conference;
 - (3) Sites required for conference; and
 - (4) Contact details for staff at all end points.

- b. The requesting party must confirm with each endpoint that they have booked the facility at their locations. The contact details are required to allow the technicians to perform pre-testing, especially if the link required has not been used before.

5. Prioritization

If operationally necessary a conference can be cancelled with no notice.

6. Registration

The registration procedure is currently being developed for use with the new Bridge.

ANNEX E

UNITED STATES VIDEO CONFERENCING NETWORK**1. National Overview**

The Defense Information Systems Agency (DISA) provides UNCLASSIFIED to Top Secret video conferencing capabilities to the Department of Defense (DOD), and it's Allies, as well as the US Federal Government, through the use of the Defense Information Systems Network (DISN) Video Services (DVS). The network is standards based H.320 compliant and supports data rates from 2 X 56/64 to 768 KBps. DVS is a worldwide service whose users access Multi-Point Control Units (MCU) located in Europe, Continental United States and the Pacific. DVS is composed of five regional hubs, each of which holds multiple DOD approved encryption equipment for classified conferencing.

The US Department of Defense recognizes Federal Telecommunications Recommendation (FTR) 1080A-1998 as the official standards-based reference document for VTC users and H.320 as the minimum acceptable standard. Conforming to these standards simply means that equipment purchased for use with the DVS Network will be able to communicate at a common level. You can download a copy of FTR 1080A-1998 from the Internet site: <http://www.ncs.gov/n2/content/standard/html/fttr.htm>

2. Hardware/Software/Firmware

Equipment used to connect to the DVS Network must, at a minimum, be capable of operating over one and two channels at quarter common intermediate format (QCIF) resolution, operate at variable rates from 56 to 1,920 kilobits per second (kbps), have a CODEC that is capable of coding at a minimum of 6 frames per second and decoding at a minimum of 7.5 frames per second. Algorithm support must be at a minimum compliant with standard H.261, and QCIF or Common Intermediate Format (CIF). QCIF and CIF define the video display with parameters such as number of lines and pixels. You may add any of the advanced capabilities that you desire such as importing video clips, computer graphics, "whiteboard" applications, or document sharing/collaboration. Be aware that the other VTFs you are conducting a conference with may not support the advanced capabilities that are available from your CODEC.

All DVS hubs are cryptographically protected utilizing cryptographic equipment approved by the National Security Agency (NSA).

The DISN Video Services worldwide architecture includes both Multi-point Control Units (MCUs) and Digital Access and Cross-connect Systems (DCCS), which makes three or more participants in a videoconference possible. Through Digital Cross Connect Switches, transmission gateways, video bridges, and crypto devices,

dedicated subscribers and dial-up subscribers are able to conduct point-to-point or multipoint VTCs classified or unclassified. Reservation scheduling can be requested by voice, fax, e-mail, web, or data transfer. DISN VTC supports tactical connections via the STEP Interface.

3. Contacts

DISN Video Services
 NS55, Sky 7
 5275 Leesburg Pike
 Falls Church, VA 22041-3801

Responsibility	Appointment	Contact Information	Remarks
Dick Mason	Deputy, DVS	Tel: 703-882-0116 Fax: 703-882-2810 E-mail: mason1d@ncr.disa.mil	Secure Fax: 703-882-3249 DSN: 312-381-0116
Wes Miller	DVS Operations	Tel: 703-681-1346 Fax: 703-681-3058 E-mail: Miller1g@ncr.disa.mil	DSN: 312-761-1346
Robert Arevalo	ARO, Information Assurance	Tel: 703-882-3248 Fax: 703-882-3249 E-mail: arevalor@ncr.disa.mil	Secure Fax: 703-882-3249 DSN: 312-381-3248
VTC Operations		Tel: 703-681-3058 Fax: 703-681-1376 E-mail: VTCOPS@ncr.disa.mil	DSN: 312-761-3058
Video Network Management Center	Alternate Bridge	Tel: 800-367-8722	AT&T Help Desk

Table E-1 Points of contact

4. National Registration Requirements

To access the DISN Video Services network you must become a subscriber, which is a two-step process. Detailed information can be found in the Newcomers Brief document. Click <http://disa.dtic.mil/disnvtc/newcomers.htm> to request the Newcomers Brief.

a. Step 1 - Ensures the connection utilizes one of the following transport standards (commercial ISDN, FTS-2001, and/or DSN Switched Digital Service) in order to interface with DVS. Individual countries should use their normal process for provisioning of the appropriate transport.

b. Step 2 - Access the Hub services that DISN Video Services provides. A Site ID (which you need to schedule a conference) is obtained by completing and submitting a Site Profile Registration.

5. Registration

(Fill out site Registration Form on-line)

General Information

When subscribers complete and submit a Site Profile Registration Form on the DISN VTC web site, they should be registering the end user device in their facility (Codec or MCU) that is the central function for a conference, with a list of maximum capabilities.

A Codec may use different forms of transport and will therefore be assigned multiple DVS Site IDs. Conference scheduling is done with only one of the DVS Site IDs.

If an MCU has more than one port assigned to DVS-G, conference scheduling can take place simultaneously on all ports. In this case, a separate Site Profile Registration Form should be used for each port (i.e., MCU1, MCU2, etc.).

Program Designator Code (PDC): _____
(This code is necessary for billing the service for CONUS/Canada customers only. For more information or assistance, contact the NS55 representative: Commercial 703-681-1376 or DSN 312-761-1376.)

If you cannot complete the Site Registration Form on-line, contact VTC OPS (Commercial 703-681-1376, DSN 312-761-1376, or VTCOPS@ncr.disa.mil).

6. Connection Approval

To obtain DVS connection at the secure level, completion of the attached Access Approval Document, as well as the Interim Authority To Operate and/or Authority To Operate letter (examples are attached), signed by the Designated Approval Authority (DAA) is required. You can download the Access Approval Document (MS Word, 83KB) from the DVS Website.

7. Reservation/Scheduling System

The DISN Video Operations Center (VOC), located at DISA CONUS, is the central scheduling location for all secure and non-secure CCEB multi-point and point-to-point videoconferences. A choice of direct or indirect methods can be used to submit your Conference Requests to the Reservation System for processing, including:

- a. AT&T Reservation Help Desk: 800-367-8722 (Direct Method)*
DSN: 312-533-3000
- b. Voice Requests: 866-228-0085
DSN 312-779-9910
- b. E-mail Requests: VTCOPS@ncr.disa.mil
- c. Fax Requests: 618-229-8688
DSN: 312-779-8688

* Direct method is utilized when a conference request is initiated within a two hour or less time frame.

Additional Information:

For additional Information please visit the DVS web site homepage at <http://disa.dtic.mil/disnvtc> or contact DSN Video Services at:

Commercial: 703-681-1376, -1346, -1368, or -1366
DSN: 312-761-1376, -1346, -1368 or -1366

E-mail: VTCOPS@ncr.disa.mil

Examples



Access Approval Document (AAD)
Must Be Completed For Cryptographic Transmission

Revised: 1 November 2002

Site ID* _____ Date _____
 Installation _____
 Location/Room # _____
 Bldg./Street _____
 City _____ State _____

This document must be completed prior to your facility being able to conduct **classified** videoconferences. Answering **No** or **not answering** any of the following questions may prevent your site from conducting classified videoconferences.

Organization Message Address _____
 i.e. DISA WASHINGTON DC//NS55//

Comsec Message Address _____

COMSEC Account # _____ LMDKP? Yes NO (ok to mark no)

CRYPTO Type: KIV-7/HS KG-194 KIV-19 **Tactical?** Yes No

Defense Courier Service (DCS) 2 line address _____

COMSEC Custodian Name _____

Phone # _____ Email _____
 COM/DSN if available

1. Provide DISA NS55 a **signed copy** of the Authority to Operate (ATO) either interim or final, a site diagram and this completed AAD.

2. Classification level: (Mark **all** that apply) Unclassified US Secret
 US Top Secret KIV-7 Allied Secret Canada

VTC Facilitator Name _____

Phone # _____ Email _____

Designated Approval Authority (DAA):

Title _____ Grade _____

E-5

ORIGINAL

Phone # _____ Email _____
COM/DSN if available
 Name _____ Signature _____ Date _____

I (DAA) certify the VTC facility listed above is authorized to operate at the requested classification level. "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."

* This must be filled in. If you currently have a site ID, enter it here. For a new Site ID please coordinate with DISN Video Services (DSN 312-761-1376, Com 703-681-1376).

Access Approval Document
 Certification / Accreditation Information
 Page 2 of 2

Designated Approval Authority:

The Designated Approval Authority (DAA) is the Command sponsored local element / entity assigned the responsibility of determining, based on the risks, if a videoconferencing system, network, or information management system can be operated in a classified mode.

You are requested to maintain this document at your site. DISN Video Services (NS55) and authorized representative (EU52 for Europe, PC52 for PAC), must have a signed copy prior to service activation and crypto key distribution.

POC for this action:

For CONUS: DISN Video Services Division (NS55), cml. (703) 882-3248, DSN 381-3248

For Europe: DISA EUR (EU52), cml. 011-49-711-68639-5955, DSN 314-434-5955

For PAC: DISA PAC (PC52), VTC OPS, cml. 808-656-0196, DSN 315-456-0196

Fax AAD, ATO and Site drawing to:

** For CONUS/OCONUS:

DISN Video Services Division (NS55)
 5275 Leesburg Pike
 Falls Church, Virginia 22041-3801
 Fax (DSN) 312-381-3249
 (Com) 703-882-3249

For EUROPE: DISA Europe/ Attn: EU52
 Unit 30403

E-6

ORIGINAL

UNCLASSIFIED

ANNEX E TO ACP 220

APO AE 09131
Fax (DSN) 314-434-5312
(Com) 011-49-711-68639-5312

For PAC: DISA PAC – Attn: PC52, VTCOPS
Bldg 107
Wright Avenue
Wheeler AAF
Hawaii 96854-5120
Fax (DSN) 315-456-3838
(Com) 808-656-3838

**** AAD is faxed to NS55 for all areas CONUS/OCONUS**

SAMPLE LETTER OF ACCREDITATION

AUTHORITY TO OPERATE (ATO)

Combatant Commander's/Service's/Agency's Name
(Address)

Date:

SUBJECT: Accreditation of Combatant Commanders/Services/Agency's Name
Workstation/network

Reference: (a) Accreditation Support Documentation

1. In accordance with the provisions of (Combatant Commander's/Service's/Agency's Name) Instruction (XXX-XXX-XX), authorization is hereby granted for the operation of the (Combatant Commander's/Service's/Agency's Name Workstation/Network), located in (Building 0000, Suite 000, Address). This accreditation is based upon a review of the information provided in reference (a). This accreditation is valid as long as the Baseline Security Safeguards defined in the (Combatant Commander's/Service's/Agency's specific security guidelines) are implemented. This system is authorized to operate in the threat environment defined in reference (a) and with stated vulnerabilities as identified in the (Combatant Commander's/Service's/Agency's) Baseline Security Documents. The accredited system consists of (list equipment here). This system is authorized to process (Place Maximum mode of operation level processed). The Combatant Commander's/Service's/Agency's workstation/network is connected to the DISN Video Services (DVS) system and (Place any other network that the system is connect to).

E-7

ORIGINAL

UNCLASSIFIED

2. This accreditation is valid for 3 years from the date of this letter. Reaccreditation is required sooner if there is any change that affects the security posture of the system. It is the responsibility of the senior official in charge of the system to ensure that any change in threat, vulnerability, configuration, hardware, software, connectivity, or other modification is analyzed to determine its impact on system security. Appropriate safeguards will be implemented to maintain a level of security with the requirements of this accreditation.

3. The undersigned accepts the risk for the operation of the Combatant Commander's/Service's/Agency's system defined above.

Signature

Designated Approving Authority
Combatant Commanders/Services/Agency's Name

Enclosure A

**SAMPLE INTERIM APPROVAL TO OPEATE
(IATO)**

Combatant Commander's/Service's/Agency's Name
(Address)

Date:

SUBJECT: Interim Approval to Operate Combatant Commanders/Services/Agency's
Name

Workstation/network

Reference: (a) Accreditation Support Documentation

1. In accordance with the provisions of (Combatant Commander's/Service's/Agency's Name) Instruction (XXX-XXX-XX), an Interim Approval to Operate (IATO) is hereby granted for the operation of the (Combatant Commander's/Service's/Agency's Name Workstation/Network), located in (Building 0000, Suite 000, Address). This IATO is based upon a review of the information provided in reference (a). This IATO is valid as long as the Baseline Security safeguards defined in the (Combatant

E-8

ORIGINAL

Commander's/Service's/Agency's specific security directives and guidelines) are implemented. This system is authorized to operate in the threat environment defined in reference (a) and with stated vulnerabilities as identified in the (Combatant Commander's/Service's/Agency's Baseline Security Documents). The IATO system consists of the (equipment list). This system is authorized to process (Place maximum mode of operation level processed). The (Combatant Commander's/Service's/Agency's) network is connected to the DISN Video Services (DVS) system and (place any other network that may be connected to).

2. This IATO is valid for 90 days from the date of this letter. Final accreditation action is required before the expiration of this IATO. This IATO will terminate sooner if there is any change that affects the security posture of the system. It is the responsibility of the senior official in charge of the system to ensure that any change in threat, vulnerability, configuration, hardware, software, connectivity, or other modification is analyzed to determine its impact on 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 (Combatant Commander's/Service's/Agency's) system defined above.

Signature

Designated Approving Authority
Combatant Commanders/Services/Agency's

Enclosure B

LIST OF EFFECTIVE PAGES

<u>Subject Matters</u>	<u>Page Numbers</u>	<u>Change in Effect</u>
Title Page	I	Original
Foreword	III	Original
CCEB Letter of Promulgation	III	Original
Record of Message Changes	IV	Original
Table of Contents	IX to X	Original
Chapter 1	1-1 to 1-6	Original
Chapter 2	2-1	Original
Chapter 3	3-1 to 3-5	Original
Chapter 4	4-1 to 4-3	Original
Annex A	A-1 to A-4	Original
Appendix 1 to Annex A	A1-1 to A1-3	Original
Annex B	B-1 to B-7	Original
Annex C	C-1 to C-3	Original
Annex D	D-1 to D-3	Original
Annex E	E-1 to E-9	Original
List of Effective Pages	LEP-1	Original

LEP - 1

ORIGINAL

UNCLASSIFIED