

DND Identification Number: 1974100118

MEMORANDUM OF UNDERSTANDING  
BETWEEN  
THE DEPARTMENT OF NATIONAL DEFENCE OF CANADA  
AND  
THE DEPARTMENT OF DEFENSE OF THE UNITED STATES OF AMERICA  
CONCERNING  
COMBINED DEFENSE INFORMATION SYSTEMS MANAGEMENT  
IN SUPPORT OF  
DEFENSE OF NORTH AMERICA  
(Short Title: CANUS CDISM MOU)

6 March 2008



County/City of Arlington  
Commonwealth/State of Virginia  
I certify this to be a complete, full, true and  
exact reproduction of the original document.  
Certified this 27th day of July, 2008  
Sandy L. Cochran  
Notary Public  
My commission expires: 30 Sept 2010

4122947

## CANUS CDISM MOU

### SECTION 1 - INTRODUCTION

1. WHEREAS the United States Department of Defense (DoD), and the Department of National Defence of Canada (DND), hereinafter referred to as the "Participants", recognize the need to continually improve telecommunication services affecting combined defense communications;

2. And WHEREAS, the U.S. Defense Information Systems Network (DISN) and the Canadian Defence Integrated Services Digital Network (DISDN) are interconnected via telecommunication gateways for the provision of secure and nonsecure voice, data and video services;

3. And WHEREAS the Participants recognize that the Agreement Concerning Cooperation in Defence Matters between the Government of the United States of America and the Government of Canada (Chapeau Agreement), dated 19 August 1993, applies to this Memorandum of Understanding (MOU).

4. Now, therefore, taking into account the foregoing, DoD and DND, have come to the following understanding:

### SECTION 2 - PURPOSE

1. The purpose of this MOU is to provide for the continuation of procedures and practices related to the establishment, operation and management of combined defense information systems; exchange of material and personnel between the Canadian Forces (CF) and the DoD Defense Information Systems Agency (DISA); and telecommunication liaison functions in Canada and the United

States pertaining to the combined defense information systems requirements and separate national defense information systems requirements.

### SECTION 3 - SCOPE

1. This MOU provides for the program implementation, configuration, engineering, and management of the Combined Military Network (CMN). The CMN includes the United States DISN covering the 48 continental states south of the Canadian border and Alaska and the Canadian DISDN in Canada. This network will be referred to hereafter in this arrangement as the CMN. The CMN provides secure and non-secure voice, data, and video services.
2. This MOU provides for combined action in maintaining effective, centralized management of the CMN to be accomplished by the Director, DISA and the DND Assistant Deputy Minister (Information Management) (ADM(IM)). (Annex A)
3. This MOU provides for the exchange of administrative, operational, and technical information, the exchange of documents and data, and for the interchange of personnel between DISA and ADM(IM). These exchanges are necessary for management, operation, and maintenance of the CMN in Canada and the United States. (Annex B)
4. This MOU provides for the activities associated with the network configuration and system engineering. The activities include program implementation, configuration, and engineering of the Defense Switched Network (DSN) and the Canadian Switched Network (CSN). (Annex C)

5. This MOU provides for the exchange of administrative, operational, and technical information, and the exchange of documents and data to provide interoperability and effective centralized management of the U.S. Defense Red Switched Network (DRSN) and Canadian Defense Red Switch Network (CDRSN). (Annex D)

6. This MOU provides for the administrative procedures and standards for secure and non-secure videoconferencing in support of the CMN. (Annex E)

7. This MOU provides for the ordering of leased facilities, services, and equipment in support of United States and Canada military telecommunications requirements. (Annex F)

8. This MOU provides for the method to be used to finance the CMN requirements in Canada and the United States. (Annex G)

#### SECTION 4 - ORGANIZATION AND TECHNICAL RESPONSIBILITIES

1. The Director, DISA, and the DND ADM(IM) will be the executive agents for this MOU. The day-to-day management activities associated with implementation of this MOU will be devolved to the DISA Principal Director for Global Information Grid Combat Support (GS) and to the DND Director General Information Management Technologies (DGIMT). The development of any further composite technical and operational proposals and procedures for telecommunications services, which may result from this MOU, will be accomplished through appropriate liaison and consultation with the Executive Agents.

2. Direct coordination between personnel of GS and those of DGIMT is authorized and encouraged. This coordination may be

accomplished by correspondence, messages, or personal visits. The minimum requirement per the Combined Defense Information Management Panel (CDIMP) Charter is an annual meeting of CDIMP panel members.

#### SECTION 5 - IMPLEMENTATION

1. In the implementation of this MOU, each Participant has overall responsibility for its own telecommunications systems, for each of the component parts of the systems and for fulfilling its own telecommunications services requirements. This responsibility includes:

- a. Carrying out and bearing the cost of procurement, installation, operation, and maintenance of equipment required; and
- b. Acquiring and bearing the cost of any services (such as leasing circuits) required in support of CMN activities.

The Participants recognize, however, that each may require assistance of the other in carrying out the tasks for which it is responsible.

2. Technical Control. Services provided will be under the technical control of the Chief, Center for Network Services (GS2) for DISA and the Director Information Management Technologies, Products and Services (DIMTPS) for DND.

3. Service Continuity. Services, once provided, will not be subject to discontinuance without the mutual consent of both Participants.

4. Circuit and Trunk Restoration Provisions. Provisions for circuit and trunk restoration will be mutually determined on a case-by-case basis. Restoration assignment policies and procedures will be determined by the providing Participant's network support center and supported by the providing Participant's technical organization.

5. Standards. Technical and compatibility standards of those facilities used will be established by the Participants.

6. Traffic Precedence. Traffic will be assigned precedence (routine, priority, immediate, flash, flash override) and will be handled over U.S. military telecommunications facilities subject to the rules and regulations that apply to U.S. military telecommunications facilities.

#### SECTION 6 - FUNDING

1. In implementation of this MOU, each Participant will bear the costs of operation and maintenance of its own telecommunications system and of meeting its own telecommunications requirements.

2. The Participants have entered into this MOU with the understanding that the exchange of telecommunications services support and related supplies and services to be undertaken pursuant to this MOU will be an exchange of equivalent value. If actual practice demonstrates that the value of the telecommunications support and related supplies and services being exchanged is not equivalent, then the Participants will enter into negotiations to adjust the arrangements so that the values remain substantially equivalent. Although unlikely, if such adjustment

is not possible, then any accrued credits and liabilities resulting from an unequal exchange of telecommunications support and related supplies and services will be liquidated by direct payment to the Participant having provided the greater amount of telecommunications support and related supplies and services, with a final liquidation made no later than 30 days after the expiration of this agreement. Annex G to this MOU outlines the financial arrangements for establishment, operation, and maintenance of the CMN.

3. Any equipment or services provided by the United States in conjunction with this MOU will be provided in accordance with the *U.S. Arms Export Control Act*.

4. This MOU is not applicable to services provided under a fee-for-service arrangement.

#### SECTION 7 - CLAIMS

1. Claims arising under this MOU will be dealt with in accordance with paragraph 1 of the Chapeau Agreement.

2. The Participants will share any costs required to be shared under subparagraph 1(b)(ii) of the Chapeau Agreement on the following basis:

a. Where responsibility for the damage, loss, injury or death, can be specifically attributed to one Participant, the cost of handling and settling the claim will be the sole responsibility of that Participant.

b. Where both Participants are responsible for the damage, loss, injury or death, the cost of handling and settling the claim will be apportioned between the Participants based on their degree of responsibility for the damage, loss, injury or death; and

c. Where it is not possible to attribute responsibility for damage, loss, injury, or death, the cost of handling and settling the claim will be distributed equally between the Participants.

3. The Participants will share any costs required to be shared under subparagraph 1(b)(iv) of the Chapeau Agreement on the following basis:

a. For contracts where one Participant contracts solely on its own behalf, the Participant awarding the contract will pay the cost of claims arising under that contract.

b. For contracts where one Participant contracts on behalf of the other Participant, the Participant on whose behalf the contract was awarded will pay the cost of claims arising under that contract. The contracting Participant will not indemnify contractors against third party liability claims, unless otherwise mutually determined; and

c. For contracts awarded on behalf of both Participants, the cost of claims arising under such contracts will be shared in the same proportions as costs are shared in the applicable follow-on arrangement. The contracting Participant will not indemnify contractors against third party liability claims, unless otherwise mutually determined.

## SECTION 8 - SECURITY

1. In order to prevent unauthorized disclosure of the other Participant's classified articles, services, documents and information, each Participant will provide substantially the same degree of security protection it would provide to protect its own classified articles, services, documents, and information of equivalent classification, bearing in mind, as a minimum, existing security arrangements and procedures prevailing between them.

## SECTION 9 - RELEASE OF INFORMATION TO THE PUBLIC

1. The release of information (formal releases or answers to queries) to the press or public concerning the arrangements and activities resulting from this MOU will be made only after being coordinated in advance. Questions addressed to one Participant concerning the activities of the other will be referred to the Participant concerned.

2. Each Participant will take all lawful steps available to keep information exchanged in confidence under this MOU free from disclosure under any legislative provision, unless the other Participant consents to such disclosure.

3. To assist in providing the desired protection, each Participant will mark such information furnished to the other with a legend indicating the country of origin, the conditions of release and the fact the information relates to this MOU and that it is furnished in confidence.

4. Unclassified information provided by either Participant to the other in confidence, and information produced by either

pursuant to this MOU requiring confidentiality will be safeguarded in a manner that ensures its proper protection from unauthorized disclosure.

SECTION 10 - REVIEW

1. The provisions of this MOU may be amended at any time by mutual written consent of the Participants thereto. The contents of this MOU should be reviewed annually by representatives of both Participants. Technical changes may be made to the Annexes without re-negotiation of the basic MOU.

2. This MOU will remain in effect for a period of five (5) years. This MOU may also be terminated by either Participant upon giving at least six (6) months written notice to the other Participant, or sooner, if mutually determined.

SECTION 11 - LANGUAGE

1. The language used in this MOU is English.

SECTION 12 - SUPERSESSSION

1. This MOU supersedes the Arrangement between the United States Defense Communications Agency and the Canadian National Defence Headquarters for the Combined Defense Information Systems Management in support of the Defense of North America, dated 1 October 1974, as amended 17 December 1975 and revised 1983, and amended on 31 August 1995.

SECTION 13 - DISPUTES

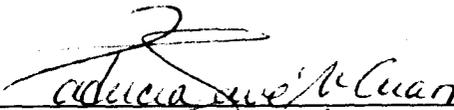
1. Any disputes resulting from the interpretation or application of this MOU will be settled by consultation only and will not be referred to a court, an international tribunal, or any other third party for settlement.

SECTION 14 - EFFECTIVE DATE

1. This Understanding, with its Annexes and Appendices as integral parts, will become effective on the date of the last signature. IN WITNESS THEREOF the undersigned, being duly authorized, have signed this Understanding.

SIGNED

For the Department of National Defence of Canada

  
\_\_\_\_\_  
PATRICIA SAUVÉ-MCCUAN  
Assistant Deputy Minister (Information Management)

at \_\_\_\_\_ Ottawa, ON  
date

For the United States Department of Defense

  
\_\_\_\_\_  
CHARLES E. CROOM  
Lieutenant General, USAF  
Director, Defense Information Systems Agency

at DISA HQ, Arlington, VA  
date 21 July 2008

Annexes: 7

- Annex A MANAGEMENT PROCEDURE
- Annex B EXCHANGE OF INFORMATION AND PERSONNEL
- Annex C NETWORK CONFIGURATION AND SYSTEMS ENGINEERING
- Annex D POLICY AND PROCEDURES FOR THE COMBINED OPERATION OF THE DEFENSE RED SWITCH NETWORK
- Annex E ADMINISTRATIVE PROCEDURES AND STANDARDS SECURE AND UNCLASSIFIED VIDEO TELECONFERENCING
- Annex F POLICY ON JOINT ORDERING OF NETWORK FACILITIES
- Annex G FINANCIAL ARRANGEMENTS

ANNEX A  
CANUS CDISM MOU

MANAGEMENT PROCEDURE

1. SCOPE. This Annex provides for combined action in maintaining an effective centralized management of the Combined Military Network (CMN) to be accomplished by the U.S. Defense Information Systems Agency (DISA) and the Department of National Defence (DND) Assistant Deputy Minister (Information Management) (ADM(IM)) Group.
  
2. GENERAL. Separate management groups will exist in both Canada and U.S. to exercise operational direction of the CMN.
  
3. MANAGEMENT POLICY - GENERAL. Policy affecting CMN operation or cost will be developed by DISA for U.S. networks and by the ADM (IM) for CF networks. These policies will be coordinated between each management agency. Policies affecting CMN operations will be issued by a DISA Circular for U.S. networks and will indicate Canadian applicability and concurrence. DND will implement a corresponding policy process.
  
4. OPERATIONAL MANAGEMENT AND PROCEDURE.
  - a. DISA will maintain total network status to provide complete system integrity with centralized operational guidance in cooperation with the ADM(IM).
  
  - b. Network administration, management, traffic data collection, routing changes, status monitoring, and application of control measures will complement each other in Canada and the U.S.

c. The U.S.-Canadian Combined Defense Information Management Panel (CDIMP) for the CMN will meet at least annually to resolve issues related to the CMN and to discuss items of mutual concern. The Panel will be comprised of senior managers from DISA and ADM(IM), and when required, those commercial carriers or their representatives who operate switches for the CMN.

5. CANADIAN SWITCHED SERVICE MANAGEMENT GROUP. Within the ADM(IM) Group, the Director Information Management Technologies, Products and Services 2 (DIMTPS 2) is designated as the Switched Services Management Group. DIMTPS 2 is the Telecommunications Services manager for the managed service contract and, as such, will:

- a. Utilize mutually determined CMN policies, which are in effect upon consummation of this MOU.
- b. Coordinate with DISA/GS23 to establish policy affecting network operation or cost, such as:
  - (1) Non-defense agency use of CMN.
  - (2) Off-net use of CMN.
  - (3) Network in-out dialing.
  - (4) Engineering criteria.
  - (5) User services.

(6) Traffic control by line load, reroute, cancel alt route, or other temporary measures as appropriate.

(7) Assistance operator procedures.

(8) Adequacy and distribution of directories.

(9) Network improvements.

(10) Telecommunication Service Renewal Project (TSRP)/Global Defence Network Services (GDNS) particulars such as non-detailed billing

c. Perform network traffic analysis for the Canadian Switched Network (CSN), and coordinate with DISA/GS23 on total system traffic analysis.

d. Perform network operational management for the CSN.

e. Perform network growth management, in coordination with DISA/GS23, as required.

f. Coordinate with DISA for user requirements, which will be homed on U.S. switches.

g. Coordinate with, or recommend as appropriate to, DISA/GS23 all necessary adjustments in trunk groups which cross the border.

6. United States Switched Service Management Group. DISA/GS23, as the United States Switched Service Management Group, will:

- a. Coordinate with DIMTPS 2 any proposed policies or policy changes which affect the overall network.
- b. Perform network management function for the CONUS Defense Switched Network (DSN).
- c. Coordinate with DIMTPS 2 for user requirements that will be homed on CSN switches.
- d. Perform network traffic analysis for the CONUS network.
- e. Coordinate with, or recommend as appropriate to, DIMTPS 2 all necessary adjustments in trunk groups.
- f. Perform total network growth management, as required, in consultation with DIMTPS 2.

ANNEX B  
CANUS CDISM MOU

EXCHANGE OF INFORMATION AND PERSONNEL

1. SCOPE. This Annex provides for the exchange of administrative, operational, and technical information, documents, and data, and for the interchange of personnel between the United States Defense Information System Agency (DISA) and the Department of National Defence (DND) Assistant Deputy Minister (Information Management) (ADM(IM)) Group.

2. GENERAL.

a. To provide for effective planning, programming, and performance of the network, it is essential that direct channels exist for the mutual exchange of information pertaining to the system.

b. The complex management aspects of a polygrid network require a closely coordinated management and control organization between the two agencies, and will, of necessity, require exchange of personnel on a continuing basis.

3. EXCHANGE OF INFORMATION, DOCUMENTS, AND DATA.

a. The Director General Information Management Technologies (DGIMT) for DND and the Principal Director for Global Information Grid Combat Support (GS) for DISA will determine the information, documents, and data necessary for management, operation, and maintenance of the CMN and will effect approval for release of material through their respective governments, to the agency concerned.

b. Information and material to be exchanged will be in categories indicated and will range from unclassified up to and including SECRET RELCAN.

c. Documents of a periodic nature will be identified and exchanged on a continuing schedule.

d. The release and handling of classified information and documents will be governed by the standard security agreements and practices prevailing between Canada and the United States.

e. The general category of information and documents to be exchanged will be those necessary for the operation, management, and engineering of the CMN to include, but not be limited to, the following voice, data, and video:

- (1) Network Configuration.
- (2) Standard Operating Procedures.
- (3) Engineering Criteria.
- (4) Traffic Studies.
- (5) Access Line and Trunk Requirements.
- (6) Restoration Plans and Priorities.
- (7) Directories

f. Any additional categories of information and documents will be mutually determined by the respective management groups.

4. EXCHANGE OF PERSONNEL.

a. Requests for personnel visits between the respective agencies will be processed through government channels for identifying data, certification of security clearances, and duration of visits. The requests then will be transmitted to the agency concerned as soon as possible prior to the proposed visit.

b. DISA and ADM(IM) will each provide two (2) officers on an exchange basis between the respective agencies.

(1) One CF exchange officer will perform assigned duties with the Center for Network Services, Defense Switched Network Division at DISA Headquarters in Falls Church, VA.

(2) One CF exchange officer will perform assigned duties with DISA Joint Interoperability Test Command (JITC), Fort Huachuca, Arizona.

(3) One DISA exchange officer will perform assigned duties with the Directorate of Information Management Technologies, Products and Services (DIMTPS) at National Defence Headquarters (NDHQ), Ottawa, Ontario.

(4) One DISA exchange officer will perform assigned duties with the Director Information Management

Engineering and Integration (DIMEI) at NDHQ, Ottawa, Ontario.

c. The CF exchange officer functions related to DISA-managed telecommunications facilities will be performed by the CF exchange officer assigned to DISA Headquarters in Falls Church, VA. The exchange officer will perform functions that will include, but not be limited to, the following:

(1) Exchange of current information on communication facilities of common interest.

(2) Coordination with DIMTPS for the purpose of obtaining telecommunications data for analysis and evaluation.

(3) Coordinating, as required, control actions relating to the Canadian Switched Network (CSN).

(4) Coordination with DIMTPS to ensure effective management of the CSN access lines.

(5) Coordination between DISA/GS23 and DIMTPS on CMN activities.

(6) Coordination with DISA/GS23 to resolve technical or transmission problems in Canada that affect operation of the CMN.

(7) Monitoring of circuit conditions and utilization of telecommunications within the CMN, and then, advising

DISA/GS23 and DIMTPS of significant trends and/or problems from circuit traffic conditions.

(8) Coordinating with DIMTPS on all cross border circuit requirements.

(9) Monitoring secure voice activities and coordinating actions related to Canadian users.

d. Requests for personnel to be assigned on an exchange basis between the respective agencies will designate the specific area of assignment, purpose, and duration of assignment. These requests will be transmitted to the agency concerned at least 180 days prior to assignment.

e. It will be the responsibility of the host agency to request extensions of the initially approved periods of assignment.

f. DISA exchange officer functions within DND will be performed by one of the DISA exchange officers, as designated, located with DIMTPS. The exchange officer will perform functions that will include, but not be limited to, the following:

(1) Exchange of current information on telecommunications facilities of common interest.

(2) Provision of technical assistance to the facility control offices and users of the U.S. Defense Information Infrastructure (DII).

(3) Assistance in planning preplanned outages.

(4) Providing prompt notification of significant items of interest such as impending labor strikes, and natural and man-made disasters affecting or that could affect telecommunications services.

(5) Other DISA matters as required by DISA Global Network Operations Security Center (GNOSC), for rapid problem solving.

5. FINANCIAL RELATIONSHIP.

a. CF exchange officers.

(1) DND will bear full responsibility for the salaries, allowances, and expenses of the CF officers.

(2) The Canadian Defence Liaison Staff (CDLS) in Washington, D.C., will supply administrative support for the CF officers.

(3) DISA/JITC and DISA Headquarters will provide travel expenses, office space, and office supplies for the respective CF officers.

b. DISA exchange officers.

(1) DoD will bear full responsibility for the salaries and allowances of the DISA exchange officers.

(2) DISA Headquarters, Arlington, VA, will provide administrative support for the DISA exchange officers.

(3) ADM(IM) will provide travel expenses, office space, and office supplies for the DISA exchange officers.

c. All administrative and financial arrangements for the exchange positions will be on a *quid pro quo* basis.

d. The directing Participant will pay all temporary duty costs, including transportation, per diem, and other allowances when exchange or liaison officers are required to travel in the course of their duties.

6. Status of officers involved in exchange functions pursuant to this MOU will be in accordance with the Agreement between the Parties to the North Atlantic Treaty regarding the Status of Their Forces dated 19 June 1951.

7. Medical coverage for exchange officers filling positions pursuant to this MOU will be provided in accordance with the Memorandum of Understanding between the Department of Defense of the United States of America and the Department of National Defence of Canada concerning Reciprocal Arrangements for the Provision of Health Care Services, dated 3 May 1993.

ANNEX C  
CANUS CDISM MOU

NETWORK CONFIGURATION AND SYSTEM ENGINEERING

1. SCOPE.

activities associated with the program implementation, configuration, and engineering of the Defense Switched Network (DSN) in the United States and the Canadian Switched Network (CSN) in Canada. These activities are to be performed by the U.S. Defense Information Systems Agency (DISA) and the Department of National Defence (DND) Director General Information Management Technologies (DGIMT).

2. GENERAL.

a. The Canadian Switched Network (CSN) consists of 6 automatic switching centers located across Canada that are provided to Bell Canada as Government Furnished Equipment (GFE) and managed by Bell Canada on behalf of the Government.

b. The United States CONUS DSN consists of 12 automatic switching centers located in the contiguous United States. The switching centers are leased by DISA from the U.S. telephone common carrier, MCI.

c. All switching centers comprising the two networks are designed to meet the DSN Generic Switching Center Requirements (GSCR), dated 8 September 2003.

d. The Combined Military Network (CMN) consists of the combined U.S. and Canadian switches and provides an improved

communication capability for DND and DoD, specifically in the areas of reliability, survivability, and flexibility.

3. NETWORK CONFIGURATION.

a. The switched network consists of three major components, all of which are compatible. These are the automatic switching equipment, transmission media, and terminal facilities. In addition, the network will have the capability to interconnect with other government and commercial networks, if and when necessary.

b. Switching centers, consisting of automatic switching equipment, provide the facilities to accept, process, and route traffic on a tandem or terminating basis. The switching center will preempt resources for lower precedence traffic to assure prompt handling of higher precedence traffic.

c. Transmission media consists of a network of cable, fiber optic, satellite, and radio facilities primarily owned by common carriers. Provision is made to use government-owned facilities where applicable. The transmission network provides the facilities for inter-switch trunks and subscribers' access lines. The inter-switch trunks will be common grade; the access lines may either use voice or special grade circuits, as required.

e. Customers connected to the switched network fall in three major categories.

(1) A Network Subscriber is any individual, installation, or activity having a direct connection to one or more switching centers.

(2) Network Users are individuals, installations, or activities that have access to one or more switching centers through a local private branch exchange (PBX) or PABX.

(3) Privileged Customer. This is a customer capable of directly calling at a precedence level higher than ROUTINE or one with inter-area calling capability.

4. SERVICES AVAILABLE. Voice services available to users will be identical throughout the network and are summarized as follows:

a. User service will provide the capability for a user to call other users or subscribers connected to the network.

b. The Privileged Customer will have the capability to exercise up to four levels of precedence, subject to the limitation of the highest precedence authorized for his use. The switching center will be programmed to recognize the highest level authorized and may be changed when required.

c. Off-hook service (hotline) is available when specifically required. An off-hook subscriber, upon lifting the handset, will be immediately connected through the switched network to a pre-designated subscriber.

d. Special purpose service features are available when specifically required. Two of the features are abbreviated dialing and preset conference.

5. CURRENT CMN CONFIGURATION.

Interoperation of the CMN is achieved with two DSN and two CSN gateway switches. For redundancy, these gateway switches provide a geographically diverse interface to each network.

6. NETWORK RECONFIGURATIONS.

a. Major reconfigurations involving the activation/deactivation of CMN switching centers will be implemented in accordance with executive agent directives.

b. Minor reconfigurations involving access line rehomings that would impact the network trunking will be implemented in accordance with executive agent directives.

7. SYSTEM ENGINEERING.

a. The CSN, as part of the U.S. Worldwide DSN, must be engineered and constructed so that standardization and uniformity is maintained. This is of the utmost importance if any degree of reliability, survivability, and flexibility is to be achieved in maintaining a network-wide capability for the transmission and completion of all offered traffic on an automatic basis.

b. To ensure that the switched network integrity is maintained for current operation and projected growth, the

engineering responsibility is vested in DISA. All requirements for switched services that are not in conformance with the GSCR should be referred to DISA for review and evaluation prior to any actions that would result in the connection of the service or services to the CMN. Direct liaison between DISA and DGIMT will be accomplished to determine if the requirement can be met and, in the event that it is not technically or economically feasible to provide the service, to develop recommendations for final resolution.

c. The user commands and agencies (DISA Joint Interoperability Test Command (JITC), DGIMT Test and Development Centre (TDC)) shall be responsible for ensuring terminal equipment (PBX, 4-wire, and others) is technically compatible and JITC-certified for interfacing with the switching centers. This requirement applies equally to leased or government-owned terminal equipment. Requirements that do not fall within these criteria should be referred to DISA for review on a case-by-case basis.

ANNEX D  
CANUS CDISM MOU

POLICY AND PROCEDURES FOR THE COMBINED OPERATION OF THE DEFENSE  
RED SWITCH NETWORK

1. SCOPE. This Annex describes the combined management activities associated with the program implementation, configuration, and engineering of the Defense Red Switch Network (DRSN) in the United States and the Canadian Defence Red Switch Network (CDRSN) in Canada. These activities are to be performed by the U.S. Defense Information Systems Agency (DISA) and the Department of National Defence (DND) Director Information Management Technologies, Products and Services (DIMTPS) on behalf of the Director General of the Information Management Operations (DGIMT).

2. GENERAL.

a. The Canadian Defence Red Switch Network (CDRSN) consists of Raytheon Red Switches delivering secure voice services to several military locations in Canada. In addition, black switches are also employed within Canada. The CDRSN is interconnected to the DRSN in the U.S. via dedicated, secure trunks. The Switches are all Raytheon Digital Small Switches and utilize Raytheon peripheral equipment to extend services where required.

b. The United States DRSN consists of many Raytheon switches located across the contiguous United States and overseas. These switches are all Raytheon technology

providing secure (up to Top Secret (U.S.)/Level III (Canada)) voice services administered by DISA.

c. The CDRSN is an adjunct of the DRSN and shares common equipment, software, and signaling protocol. DISA ensures that equipment and software provided to Canada are current, compliant, and ensure interoperability.

3. PROCEDURES.

a. U.S. Northern Command (NORTHCOM) is the sponsor for the CDRSN.

b. DISA is the focus for all Foreign Military Sales (FMS) and FMS Amendments (procurement) for the CDRSN. Acquisition of CDRSN components and their sustainment, training, life-cycle management, and support will be managed by DIMTPS and provided to Canada through DISA.

4. NETWORK MANAGEMENT.

a. For the CDRSN, the DGIMT is the authority for the management of the CDRSN network. The CDRSN Life Cycle Material Manager (LCMM), within DIMTPS, provides life cycle management, technical support and network design.

b. DISA is the management authority for the DRSN.

c. The CDRSN is monitored by the CF Network Operations Centre (CFNOC) using the Advanced Red Defense Information Management Support System (ARDIMSS). The ARDIMSS in use

within Canada is identical in operation to the U.S. system but is operated independently.

5. CONFIGURATION MANAGEMENT.

a. The DISA DRSN Single System Manager (SSM) provides operational direction, management control and technical guidance for the DRSN. The functional equivalent for the CDRSN is DGIMT / DIMTPS / LCMM. The CDRSN LCMM Position has been established within DIMTPS 2-2 and is focal point for CDRSN configuration management.

b. DGIMT: Changes and services provided by the CDRSN will be requested through the Request For Service (RFS) process. A Request for Change (RFC) will be submitted to the Information Management Configuration Control Board (IMCCB) for assessment and approval. Configuration Management issues are administered in accordance with the CDRSN Configuration Management Plan, Version 2.0 / August, 2003.

6. SECURITY.

a. Security requirements for the DRSN are published in a DISA circular DISA 300-115-7 (Final Draft / 2002-11-07) Defense Red Switch Network (DRSN) Security Guide. CDRSN installations comply with the security requirements as outlined plus the requirements as stipulated in the DND / CF - Security Orders and Directives for Classified Information Systems (Interim 2002-03-01). The DGIMT document CDRSN Security Concept Of Operations, Version 2.1/ September 2003 describes the security process as it applies to the CDRSN.

b. The CDRSN National Information System Security Officer (ISSO) is the focal point for all security issues pertaining to this network.

c. The Director Information Management Security (D IM SECUR) is the DND authority for security assessment of the CDRSN, including the approval of Interim Authority to Process (IAP) and Authority to Communicate. A Technical Communications Security (COMSEC) Inspection (TCI) is required and an Approval to Process (IAP or AP) will be provided from the D IM SECUR authority prior to any connections to the CDRSN being made.

7. TRAINING. Initial training for CDRSN technical support and the system users has been carried out by Raytheon as part of the implementation activity. CDRSN LCMM is responsible for providing a training plan and for ongoing training.

8. FINANCE.

a. DoD and DND will each bear the costs of site preparation, installation, recurring, and maintenance for their respective secure voice terminals and switches.

b. DoD and DND will each be responsible for procuring telecommunication circuits from termination to Canadian-United States cross-border points, as well as, pay for the lease installation and recurring costs within their respective territories. It will be mutually determined between DISA and DGIMT which common carrier border connection points will be used.

9. LOGISTICS.

Logistics support for the CDRSN is the responsibility of the DGIMT with assistance from DISA.

ANNEX E

CANUS CDISM MOU

ADMINISTRATIVE PROCEDURES AND STANDARDS FOR  
SECURE AND UNCLASSIFIED VIDEO TELECONFERENCING

1. SCOPE. This Annex provides the administrative procedures, standards, configuration control, and security of the video teleconference (VTC) connectivity between the Participants.

2. GENERAL. The Participants should incorporate the administrative procedures and standards identified in this appendix in its respective VTC network's Standard Operating Procedure (SOP) and Security Orders (SO), as appropriate. Defense Information Systems Network (DISN) Video Services (DVS) is the video transfer portion of the DISN. It supports global VTC requirements from CONTROLLED UNCLASSIFIED through COLLATERAL TOP SECRET classification levels.

a. This Annex addresses specific VTC connection requirements for DVS by DND under the auspices of the U.S.-Canada Combined Defense Information Management Panel (CDIMP). This process is amplified in the DISA DVS Connection Approval Process (CAP) document.

b. The CDIMP framework will be applied to meet the requirements below to obtain an Authorization To Connect (ATC) for Department of National Defence (DND) VTC sites to the DVS portion of the DISN at both the Unclassified and ALLIED SECRET Classification levels.

c. An evaluation of customer documentation will be performed to determine if required criteria are met. System testing is required and database management provides status information on the approval process and customer base.

3. SYSTEM CONNECTION REQUIREMENTS - The Initial Contact, DVS Registration, Authority To Connect Request, Authority to Operate Letter, Access Approval Document, Video Teleconferencing Facility (VTF) Connectivity and Configuration Diagram and DD Form 2875 to be completed, are all identified in the DISA DVS CAP.

4. PROCESSING DVS PACKAGES - After all required information has been submitted to DIMTPS, each DVS request package will be reviewed, coordinated with DISN Video Services at DISA, entered into the Video Services database, and forwarded to DVS for continued processing. All required documents outlined in the DVS Connection Approval Process must be provided to the DISN Video Services Program Management Office (DVS PMO).

5. REPORTING SYSTEM CHANGES - When any significant change is made to a system that connects to DVS, such as accreditation status, security posture, foreign access, and/or backdoor/backside commendations, the responsible commander must submit appropriate information to DIMTPS for validation and furtherance to the DISN Video Services Division.

6. DVS TERMINATION - The Chief, Center for Network Services (GS2) 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. In the case

of DND sites this right of denial will be staffed bilaterally prior to discontinuation of service, however, final authority for access to DVS rests with GS2.

7. RISK REVIEW - Any DVS connection that, in accordance with the DVS connection and approval process, introduces unacceptable risk must be reviewed by the DISN Security and Accreditation Working Group (DSAWG) and DIMTPS on behalf of the DND sites. Commanders responsible for DVS terminals that exhibit unacceptable risk will be notified by DIMTPS after receiving notification through GS2.

8. SECURITY AWARENESS AND TRAINING - Security training and awareness programs must be conducted according to guidance applicable to the local support.

ANNEX F  
CANUS CDISM MOU

POLICY ON JOINT ORDERING OF NETWORK FACILITIES

1. SCOPE. This Annex provides for the ordering of leased facilities, services, and equipment in support of the Combined Military Network (CMN) requirements in Canada and the United States.
  
2. GENERAL. Because of economies available under current bulk ordering arrangements, the Department of Defense (DoD) and the Department of National Defence (DND) will each order and pay for services from the U.S.- Canadian border to the terminal location within their respective country.
  
3. PROCEDURE
  - a. Prior to ordering cross-border services, the Defense Information Systems Agency (DISA) and the Assistant Defense Minister (Information Management) (ADM(IM)) group will coordinate and determine the technical and administrative details of the requirement. When concurrence is reached, the U.S. DoD and DND Canada Telecommunications Service Management Groups will place the requirement with the Defense Information Technology Contracting Office (DITCO) and the Director Information Management Technologies, Products and Services 2 (DIMTPS 2) respectively, for action.
  
  - b. Leasing action will be accomplished by DITCO and DIMTPS 2 in accordance with existing detailed procedures. The details of these procedures may be changed by mutual

agreement between the leasing agencies of each Participant without change to this document.

c. A DIMTPS/DITCO annual meeting can be arranged to review leased facilities performance to enhance any procedural anomalies.

ANNEX G  
CANUS CDISM MOU  
FINANCIAL ARRANGEMENTS

1. SCOPE. This Annex outlines the method to be used to finance the CMN. The financial procedures contained herein do not affect existing arrangements for cost sharing of Combined U.S. and Canadian Air Defence requirements covered separately under the agreements between the Royal Canadian Air Force and the United States Air Force for the Sharing of Costs of Operation and Maintenance of Improvements in the Continental Air Defense System, dated 27 September 1961; the Sharing of Costs of Communications Facilities, dated 7 October 1965; the exchange of notes on the Cost Sharing of Operation and Maintenance of the Pine Tree Radar Stations in Canada, dated 16 August 1971; Supplementary Arrangement between the United States Air Force and the Canadian Forces on Operations Maintenance and Support of the North Warning System, dated 12 December 1988, and as subsequently revised.

2. GENERAL. To provide effective planning, programming, budgeting, and accounting for the financial resources necessary to support the CMN, it is essential that financial arrangements clearly identify funding responsibilities for switched networks (voice, data, video).

3. BACKBONE NETWORK COSTS. The backbone network is defined as the switching centers and interconnecting trunks. The DoD will finance the costs of all intra-U.S. trunks and cross-border trunks up to the border crossing point with Canada and the DND

will finance the costs of all intra-Canada trunks and cross-border trunks up to the border crossing point with the U.S. Each Participant will also finance the costs for switching centers located in their respective territories. Specifically:

- a. The DoD will finance the operation and maintenance of the CONUS Defense Switched Network (DSN) and the CONUS Defense Red Switched Network (DRSN).
- b. DND will finance the operation and maintenance of the Canadian Switched Network (CSN) and the Canadian Defense Red Switched Network (CDRSN).
- c. Each Participant will also be responsible for financing any costs associated with providing additional routing trunks within its borders that may be required to support the CMN. Dedicated private lines for one Participant are the responsibility of that Participant.

4. ACCESS LINE COSTS. Access lines are defined as circuitry connecting a subscriber terminal with a switch. Each subscriber will finance the cost of his access line to include terminal cost and any costs, initial or continuing, for connection into the switches, including any special equipment and termination charges. Any access lines that cross the US-Canada border will be funded like the backbone trunking, so that each participant to pay for the portion of the circuit on their side of the border.

FINANCIAL SETTLEMENT. The Participants understand that the continuation of the procedures and practices related to establishment, operation, and management of the CMN is in both Participants' national interest and that the value of the reciprocal support each provides under this MOU for the benefit of the other to ensure interconnectivity results in an equivalent value exchange. Specifically, the costs associated with the responsibilities each Participant undertakes in paragraphs 3 and 4 of this Annex will result in an exchange of equivalent value. For the purpose of this MOU, equivalent access for both Participants to the other Participants' networks will be considered an equivalent value, regardless of the number of calls placed by either Participant or the aggregated call statistics. That is, equivalent value is based on having the capability to access the other Participant's network, regardless of how much this access is used.