

AMENDMENT NUMBER ONE TO THE
MEMORANDUM OF UNDERSTANDING

AMONG

THE MINISTER OF NATIONAL DEFENCE OF CANADA

THE MINISTER OF DEFENCE OF THE FRENCH REPUBLIC

THE FEDERAL MINISTRY OF DEFENCE OF

THE FEDERAL REPUBLIC OF GERMANY

THE MINISTER OF DEFENCE OF THE REPUBLIC OF ITALY

THE MINISTER OF DEFENCE OF THE KINGDOM OF THE NETHERLANDS

THE MINISTRY OF DEFENCE OF THE KINGDOM OF NORWAY

THE SECRETARY OF STATE FOR DEFENCE OF THE UNITED KINGDOM

OF GREAT BRITAIN AND NORTHERN IRELAND

AND

THE SECRETARY OF DEFENSE ON BEHALF OF THE DEPARTMENT OF


DEFENSE OF THE UNITED STATES OF AMERICA

FOR

INTEROPERABLE NETWORKS FOR SECURE COMMUNICATIONS

(SHORT TITLE: INSC)

Certified to be a true copy:



Diane Gaspar
International Agreements Specialist
Navy International Programs Office

AMENDMENT NUMBER ONE TO THE
MEMORANDUM OF UNDERSTANDING

AMONG

THE MINISTER OF NATIONAL DEFENCE OF CANADA

THE MINISTER OF DEFENCE OF THE FRENCH REPUBLIC

THE FEDERAL MINISTRY OF DEFENCE OF

THE FEDERAL REPUBLIC OF GERMANY

THE MINISTER OF DEFENCE OF THE REPUBLIC OF ITALY

THE MINISTER OF DEFENCE OF THE KINGDOM OF THE NETHERLANDS

THE MINISTRY OF DEFENCE OF THE KINGDOM OF NORWAY

THE SECRETARY OF STATE FOR DEFENCE OF THE UNITED KINGDOM

OF GREAT BRITAIN AND NORTHERN IRELAND

AND

THE SECRETARY OF DEFENSE ON BEHALF OF THE DEPARTMENT OF

DEFENSE OF THE UNITED STATES OF AMERICA

FOR

INTEROPERABLE NETWORKS FOR SECURE COMMUNICATIONS

(SHORT TITLE: INSC)

INTRODUCTION

1. The purposes of Amendment Number One to the Memorandum of Understanding among the Minister of National Defence of Canada, the Minister of Defence of the French Republic, the Federal Ministry of Defence of the Federal Republic of Germany, the Minister of Defence of the Republic of Italy, the Minister of Defence of the Kingdom of The Netherlands, the Ministry of Defence of the Kingdom of Norway, the Secretary of State for Defence of the United Kingdom of Great Britain and Northern Ireland, and the Secretary of Defense on behalf of the Department of Defense of the United States of America for Interoperable Networks for Secure Communications (INSC MOU) are to:

- a. Add additional work to the scope of work and increase the contributions for the INSC MOU; and
- b. Extend the term of the INSC MOU for an additional year.

2. Accordingly, the Minister of National Defence of Canada, the Minister of Defence of the French Republic, the Federal Ministry of Defence of the Federal Republic of Germany, the Minister of Defence of the Republic of Italy, the Minister of Defence of the Kingdom of The Netherlands, the Ministry of Defence of the Kingdom of Norway, the Secretary of State for Defence of the United Kingdom of Great Britain and Northern Ireland, and the Secretary of Defense on behalf of the Department of Defense of the United States of America have reached the following understandings:

AMENDMENT

The INSC MOU is hereby amended as follows:

1. TABLE OF CONTENTS

- a. Annex A title: Change the Annex A title to read:

"ANNEX A INSC PHASE I TASK DESCRIPTIONS"

- b. After the Annex A title, add the following new entry to the Table of Contents:

"ANNEX B INSC PHASE II TASK DESCRIPTIONS"

2. SECTION I, DEFINITIONS OF TERMS AND ABBREVIATIONS

- a. Definition of Project Plan: Replace the first sentence of the current definition with the following:

"A two-part document, one part developed during INSC Phase I and the other part developed during INSC Phase II, which is approved by the Steering Committee (SC) and which shows the details of the integrated tasks, schedule and resources required to accomplish the objectives of this MOU."

- b. Definition of Service Level Agreement: Add the following new definition after the definition of Project Plan:

"Documentation of understandings between different network providers or between a network provider and a user with respect to quantitative measures of service quality provided."

- c. Paragraph 1.2, Abbreviations: Insert the following abbreviations and their corresponding terms in the list of abbreviations:

"BGP-4	Border Gateway Protocol-4
COTS	Commercial Off The Shelf
DVB	Digital Video Broadcast
IPv4	Internet Protocol, version 4
MIPv6	Mobile Internet Protocol, version 6
NB	Narrow Band
PKI	Public Key Infrastructure
SLA	Service Level Agreement
TCP	Transmission Control Protocol
WAN	Wide Area Network
WBS	Work Breakdown Structure"

3. SECTION III, SCOPE OF WORK

- a. Paragraph 3.2: Replace Paragraph 3.2. with the following new Paragraph 3.2.:

"The overall work performed under Phase I of this Project will consist of eight separate task areas. A short description of these task areas is provided below. Annex A (INSC Phase I Task Descriptions) provides additional detail to these tasks."

- b. Paragraph 3.2.1: In the last sentence, add the words, "the INSC Phase I" in front of the words, "Project Plan", and add the words, "INSC Phase I" in front of the words, "final Project report".

- c. Add the following new paragraph 3.3, and renumber current paragraph 3.3:

"3.3. The overall work performed under Phase II of the Project will consist of five separate task areas. A short description of these task areas is provided below. Annex B (INSC Phase II Task Descriptions) provides additional detail to these tasks.

3.3.1. Task 1: Architecture -- This task will entail the technical management, including planning and coordination, of the INSC Phase II. This task will develop the functional and test requirements of the architecture for the INSC Phase II WAN. This will provide the framework for the integration of the work to be carried out in Tasks 2 through 5, and will develop the INSC Phase II part of the Project Plan. Subject to SC review and approval, this task will involve also the reporting and dissemination of the results of INSC Phase II during and upon completion of the Project, and the development of the INSC Phase II final Project report.

3.3.2. Task 2: Security -- This task will determine, investigate and demonstrate additional security mechanisms to be applied in INSC Phase II. The task will focus on IPsec multicast, tactical PKI, management and security, and an IPsec discovery protocol. Security products will be selected, developed, or modified if necessary, and implemented in the INSC network.

3.3.3. Task 3: Mobility -- This task effort will address network mobility of both edge systems and portions of an IP networking infrastructure. Areas for detailed study in the INSC Phase II effort will include: assessment of technology suitability and maturity, improved auto configuration and access control, performance evaluation, and analysis of interoperability with existing infrastructures. This task will demonstrate prototype software and will perform experiments and analysis of related functionality within a coalition environment.

Task 3: Mobility								
Design	X	X	X	X	X	X	X	X
Implementation	X	X	X	X		X		X
Testing	X	X	X	X	X	X	X	X
Task 4: Network and Traffic Management								
Design	X	X			X	X	X	
Implementation							X	X
Testing	X	X	X	X	X	X	X	X
Task 5: Wide Area Networking and IPv4/IPv6 Interworking								
Design	X	X	X	X	X	X	X	X
Implementation	X	X	X	X	X	X	X	X
Testing	X	X	X	X	X	X	X	X

5. SECTION V, MANAGEMENT (ORGANIZATION AND RESPONSIBILITIES)

- a. Paragraph 5.3.3: Replace Paragraph 5.3.3. with the following new Paragraph 5.3.3:

“Reviewing the technical progress of the Project against Annex A (INSC Phase I Task Descriptions) and Annex B (INSC Phase II Task Descriptions) and the Project Plans.”

6. SECTION VII, FINANCIAL PROVISIONS

- a. Paragraph 7.2: Insert the following title above the existing contribution table in Paragraph 7.2:

“INSC Phase I Contributions”

- b. Add the following new contribution table after the subparagraph that begins with the words, “For Participants other than ...”, and ends with the words, “conversion to the Euro.”:

INSC Phase II Contributions

Participant	National Contribution in National Currency
Canada	0.75M CA\$
France	1.50M Euro
Germany	1.70M Euro
Italy	1.20M Euro
The Netherlands	0.40M Euro
Norway	5.00M NOK
United Kingdom	0.60M GBP
United States	2.00M US\$

7. SECTION XI, SECURITY

- a. Paragraph 11.1: In line six, replace "C-M(55)15 (Final) of 15 October 1997" with "C-M(2002)49 dated 17 June 2002"

8. SECTION XIX, EFFECTIVE DATE

- a. Paragraph 19.1: Replace Paragraph 19.1. with the following new Paragraph 19.1:

"This MOU consists of Sections I to XIX and two Annexes. It becomes effective when it has been signed on behalf of all the Participants upon the date of the last signature and unless terminated or extended by the written consent of the Participants, will remain in effect for six years."

9. ANNEX A

- a. Title for Annex A: Change the title to read:

"ANNEX A: INSC PHASE I TASK DESCRIPTIONS"

- b. Annex A table of contents, Appendix 1: Change the title to read:

"Appendix 1 INSC Phase I schedule"

- c. Introduction: Replace the first sentence of the first paragraph of the Introduction with the following:

"The work under the MoU for INSC Phase I will provide a demonstration of a secure, loosely coupled military internetwork, as applied to a variety of transmission media."

- d. Introduction: Replace the second sentence of the second paragraph of the Introduction with the following:

"The work to be carried out under INSC Phase I is broken down into 8 tasks, as follows:"

- e. Task 1 -- System Architecture: In Paragraph 2.2, in the fourth line, add the words, "INSC Phase I part of the" before the words, "Project plan"; and in the last line, after the words, "INSC final report", add the words, "for INSC Phase I."

10. ANNEX B

a. Add the following new Annex B:

"ANNEX B: INSC PHASE II TASK DESCRIPTIONS

1. Introduction
 2. Architecture
 3. Security
 4. Mobility
 5. Network and Traffic Management
 6. Wide Area Networking and IPv4/IPv6 Interworking
- Appendix 1 INSC Phase II schedule

1. INTRODUCTION

The work under the MoU for INSC Phase II will provide a demonstration of a secure, loosely coupled military internetwork, as applied to a variety of transmission media. The envisaged operational benefits which will accrue from this work are

- timely command decisions
- consistent tactical picture
- transmission of high volume surveillance information
- time-critical weapons targeting and control
- improved quality-of-life to deployed personnel

A coordinated multinational program of work will be carried out to set up and run the INSC Phase II. The work to be carried out under INSC Phase II is broken down into 5 tasks, as follows:

Task 1 – Architecture

Task 2 – Security

Task 3 – Mobility

Task 4 – Network and Traffic Management

Task 5 – Wide Area Networking and IPv4/IPv6 Interworking

The work to be carried out by the Participants under each task is described in paragraphs 2 through 6 of this Annex.

2. TASK 1 – ARCHITECTURE

2.1 Description

This task will be responsible for the technical management, including planning and co-ordination, of INSC Phase II.

The task will develop the functional and test requirements of the architecture for the INSC Phase II WAN. This will provide the framework for the integration of the work to be carried out by Tasks 2 to 5.

Subject to SC review and approval, this task will also be responsible for the reporting and dissemination of the results of INSC Phase II during and upon completion of the project, and the development of the INSC Phase II final Project report.

2.2 Products

The following deliverables will be provided:

- INSC Phase II part of the Project plan (incl. WBS)
- WAN architecture
- Test and demonstration plan and schedule
- INSC Final report for Phase II.

3. TASK 2 – SECURITY

3.1 Description

This task will determine, investigate and demonstrate additional security mechanisms to be applied in INSC Phase II. The task will focus on IPSec multicast, tactical PKI, management of security and an IPSec discovery protocol, which were not in INSC Phase 1. Security products will be selected, developed, or modified if necessary, and implemented in the INSC network. Co-ordination with other tasks, such as Task 4 – Network and Traffic Management will be performed. The output from this task will be technology and new features for developers of IPSec devices.

Since the IPSec framework was designed to protect any kind of IP traffic, it can be used in particular for secure multicast communication. Problems that arise in the fields of negotiation and management of the security parameters and the dynamics of communication groups will require resolution.

INSC Phase I showed the general need to introduce a tactical PKI. Since the management of security is currently complex, new approaches have to be investigated that will facilitate co-ordination of security management across a coalition network of networks.

The IPSec specifications will not define a protocol for discovering the destination IPSec device. In INSC Phase I, static tunnels were used to connect two IPSec devices with no option to dynamically select an alternate IPSec device. For larger and more dynamic networks this mechanism should be replaced by an IPSec discovery protocol.

3.2 Products

The following deliverables will be provided:

- Determination of functional requirements for using IPsec multicast in coalition networks.
- Robust mechanisms for security parameter negotiation and group management. Because of the large variety of group communication scenarios, restriction to a single solution might not be sufficient to achieve secure IP multicast in every case.
- Introduction, specification and demonstration of a tactical PKI.
- Selection of suitable products and demonstrate policy-based access control.
- Definition and implementation of a discovery protocol for IPsec in order to choose correct destination IPsec device in a large dynamic coalition network.

4. TASK 3 – MOBILITY

4.1 Description

This task effort addresses network mobility of both edge systems and portions of an IP networking infrastructure. Areas for detailed study in the Phase II effort will include: assessment of technology suitability and maturity, improved auto configuration and access control, performance evaluation, and analysis of interoperability with existing infrastructures. This subtask will demonstrate prototype software and will perform experiments and analysis of related functionality within a coalition environment. The output for this task will be recommendations and technical solutions relating to the use and suitability of this technology area to military applications. Subtasks will include:

4.1.1 Task 3.A: Edge System Mobility

While INSC Phase I efforts successfully demonstrated the suitability of basic edge system mobility for the military environments, also it became clear that for deployment in real operational scenarios, a more enhanced functionality is needed. Research and investigations in INSC Phase II will address issues like system auto configuration, MIPv6 performance enhancement, and possible support for IPv6 networks in motion.

4.1.2 Task 3.B: Mobile Ad Hoc Networking (MANET)

MANET routing is next generation IP technology that provides needed support for wireless areas of a network that contains dynamic links and potentially supports mobile routing nodes. A direct output of this effort will be improved MANET technology, including auto configuration and multicast capabilities not previously available. Also the effort will provide recommended techniques for

deploying MANETs in a coalition environment (e.g. improving network survivability and distributed operation).

4.1.3 Task 3.C: Wireless Technologies and Mobile Networking

This task will examine alternative wireless technologies and techniques with respect to mobile application scenarios, involving MANET and MIPv6. Possible demonstration enhancements include power amplification for increased link range and transverter technology to allow operation within military frequency bands. Some Participants also will examine tactical wireless technologies and related mobile performance issues. The outputs of this subtask will be potential demonstrations and simulations to evaluate performance and suitability for the integration of various wireless technologies used in conjunction with INSC mobility solutions.

4.2 Products

The following deliverables will be provided:

- Enhanced MIPv6 Mechanisms and Procedures
- MIPv6 Access Control and Advanced Auto configuration Methods
- Hierarchical MIPv6 Architectural Recommendations
- Aggregate Network Mobility Technology Recommendations
- Enhanced MANET Mechanisms
- MANET Prototypes for Heterogeneous Operating Systems and Portable Devices
- MANET Access Control and Advanced Auto configuration Methods
- MANET Multicast Routing Mechanisms and Recommendations
- Recommendations and Procedures for Use with Various Wireless Technologies.

5. TASK 4 – NETWORK AND TRAFFIC MANAGEMENT

5.1 Description

Whereas in INSC Phase I network management was limited to the management of fixed networks within separate security domains, in INSC Phase II coalition network management solutions will be demonstrated for the more difficult case where:

- the network-of-networks being managed spans multiple security domains;
- the architecture includes mobile ad-hoc networks;
- users may roam between networks and need to have access, authentication and accounting mechanisms established for them across the whole coalition infrastructure;

- quality of service needs to be managed end-to-end both at the network level and at the user-service level; or
- there is a need for dynamic solutions that support changes to network topology and loading during different phases of military operations and which are robust to attack.

Among the approaches to be considered to meet these requirements will be:

- Policy Based Network Management (PBNM)
- dynamic SLAs
- new protocols for QoS management.

5.1.1 Task 4.A Management concepts and architecture

This subtask will identify solution concepts for coalition network management. It will develop representative scenarios with multiple security domains, mobile networks and roaming users. It will provide overall co-ordination and planning for the following subtasks.

The aim will be to define management processes that will enable rapid deployment of a coalition network, using automation and standard procedures to reduce the demand for skilled manpower. The concept is to use dynamically negotiated SLAs and policy statements in place of detailed configuration instructions.

5.1.2 Task 4.B: QoS and service management

To efficiently provide end-to-end QoS in response to changing operational needs, all the routers have to be quickly reconfigured. This must be achieved consistently and coherently to ensure predictable and repeatable behaviour. This is possible only if the configuration is applied by the Network Management system. The suitability of available PBNM products will be investigated.

Coalition networks will consist of a combination of national networks, coalition owned networks, and network services provided by external network service providers. In order to ensure a stable and predictable operating environment, the network services delivered by each of the Participants must comply with an SLA which will include QoS aspects. A military service level specification must take into account the dynamic nature of tactical and operational military networks. Where the coalition WAN is supporting multiple security domains including national as well as coalition LANs, the SLA for each LAN/WAN gateway will define the QoS to be provided by the WAN. Methods are needed to ensure that the WAN can provide to all users the requisite service specified in the SLAs. This subtask will investigate and demonstrate how SLAs should be defined, monitored and dynamically modified in the military coalition scenario.

This sub-task will also investigate how information transfer services (e.g. messaging/e-mail, voice, web browsing) and specific information systems are managed, to ensure that the service quality, as perceived by the users, matches their expectations. Studies on Service Level Management will consider how a service should be defined, and how best to monitor to ensure that the service is working as expected. If suitable products can be found, these studies will lead to demonstration of technology for monitoring and proactively managing system resources to optimise information service operation.

5.1.3 Task 4.C. Security of Management

It is essential that the network management system is itself secure, in order to ensure the integrity of the network service. It is particularly difficult to ensure security of the overall network management system where a coalition network is provided using component networks in different security domains.

The work in INSC Phase 1 will be extended to demonstrate a security guard function capable of filtering network management information at a security boundary between networks.

5.2 Products

The following deliverables will be provided:

- concepts and management processes for rapid deployment of a coalition network
- evaluation of PBNM for end-to-end QoS management
- recommendation on how SLAs should be defined, monitored and dynamically modified in the military coalition scenario
- demonstration of technology for monitoring and proactively managing system resources to optimise information service operation
- demonstration of a security guard function capable of filtering network management information

6. TASK 5 – WIDE AREA NETWORKING AND IPv4/IPv6 INTERWORKING

6.1 Description

This task will be responsible to develop, build, maintain and improve the INSC Wide Area Networks according to the requirements set by the other tasks. This task has also to provide the interworking capabilities in order to support both IPv6 and IPv4 information services on the same network infrastructure.

Building on the INSC Phase 1 WANs, Task 5 will particularly contribute by new developments to the following items:

- SATCOM: integration of DVB technologies into INSC Networks infrastructure

- Narrow Band Links and Subnets: development of NB links traffic control devices in the red domain
- Dual BGP-4 Autonomous System Gateways: design and configuration of multiple BGP4 Gateways in order to optimize the use of traffic resources
- Reliable Multicast: Develop methods for forming multicast groups and demonstrate reliable delivery with TCP friendly flow control
- Load Distribution: definition of methods and procedures for directing traffic to maximize the use of all available links
- Interworking of IPv4 and IPv6 information services: configuration and integration of Network Address Translators and Application Level Gateways in order to support the use of legacy IPv4 applications over the IPv6 INSC infrastructure.

6.2 Products

The following deliverables will be provided:

- Naming and Addressing Plan
- Configuration Plan
- Networks Topology
- SATCOM Connectivity Integration and Test Plan
- Mechanism and software to handle Narrow Band Links
- Narrow Band Links Integration and Test Plan
- Wide Area Networks Integration and Test Plan
- Routing Configuration Procedures
- NAT (Network Address Translator) and ALG (Application Level Gateway) Configuration Guidelines.