INFORMATION ASSURANCE FOR ALLIED COMMUNICATIONS AND INFORMATION SYSTEMS

ACP 122(F)

COMBINED COMMUNICATIONS-ELECTRONICS BOARD (CCEB)

DECEMBER 2008

FOREWORD

1. The Combined Communications Electronics Board (CCEB) is comprised of the five member nations, Australia, Canada, New Zealand, United Kingdom and United States and is the Sponsoring Authority for all Allied Communications Publications (ACPs). ACPs are raised and issued under common agreement between the member nations.

2. ACP 122(F), INFORMATION ASSURANCE FOR ALLIED COMMUNICATIONS AND INFORMATION SYSTEMS is an UNCLASSIFIED CCEB publication. This ACP should be read in conjunction with the ACP 133 Supp-1.

3. This publication contains Allied military information for official purposes only.

4. It is permitted to copy or make extracts from this publication.

5. This ACP is to be maintained and amended in accordance with the provisions of the current version of ACP 198.

THE COMBINED COMMUNICATION-ELECTRONICS BOARD LETTER OF PROMULGATION

FOR ACP 122(F)

1. The purpose of this Combined Communication-Electronics Board (CCEB) Letter of Promulgation is to implement ACP 122(F) within the Armed Forces of the CCEB Nations. ACP 122(F), INFORMATION ASSURANCE FOR ALLIED COMMUNICATIONS AND INFORMATION SYSTEMS, is an UNCLASSIFIED publication developed for Allied use 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 122(F) is effective upon receipt for CCEB Nations. NATO Military Committee (NAMILCOM) will promulgate the effective status separately for NATO Nations and Strategic Commands. ACP 122(F) will supersede ACP 122(E), which shall be destroyed in accordance with national regulations.

EFFECTIVE STATUS

Publication	Effective for	Date	Authority
ACP 122(F)	CCEB	On Receipt	LOP

3. This ACP will be reviewed periodically as directed by the CCEB Permanent Secretary.

4. All proposed amendments to the publication are to be forwarded to the national coordinating authorities of the CCEB or NAMILCOM.

For the CCEB Principals:

John Stott

JA STOTT
Lt Cdr RN
CCEB Permanent Secretary

RECORD OF MESSAGE CORRECTIONS

Identification of Message Correction and Date Time Group (DTG)		Date Entered	Entered by (Signature, Name, Rank, Grade or Rate and Name of Command)
DTG	Correction		

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

BACKGROUND

101. Collaborative international military activities are increasingly introducing requirements for the interconnection and interoperation of Defence Communications and Information Systems (CIS) operated by the participating nations. The interconnection of CIS controlled by different authorities requires the identification and reconciliation of any differences in security policy and practices among those authorities.

PURPOSE

102. ACP 122(F) is produced to establish the framework to facilitate the interconnection and interoperation of CIS between the Combined Communications-Electronics Board (CCEB) nations, and, where necessary, to support the development of Allied Information Assurance (IA) agreements. It defines the IA policies, procedures and doctrine to enable a secure combined information environment.

SCOPE

103. The approach advocated in this document calls for the recognition of minimum baseline security requirements that must be imposed on combined CIS and Nationally Affiliated Systems (NAS), and on the application of additional security measures beyond these minimum requirements when justified through risk assessment. This publication applies to all combined and shared CIS that process, store, distribute or communicate unclassified, classified or otherwise sensitive information. Combined CIS are those that process, store, distribute or communicate information shared among two or more nations. Shared CIS are CIS which process, store and transmit shared information and over which participating member nations share the responsibility for operation of the CIS. This Allied Communication Publication (ACP) applies to new and existing systems, regardless of the level of command responsible for system planning, implementation and operation.

APPLICATION

104. This publication applies to all CCEB member nations who have ratified and adopted this publication for use.

RESPONSIBILITIES

105. The following organisations are described to show their responsibility:

a. **Combined Communications Electronics Board (CCEB).** The CCEB is a five-nation joint military communications-electronics Organisation whose mission is the coordination of any military Communications and Electronics matter that is referred to it by a member nation. Its role is to examine military Communications and Electronics issues to ensure allied interoperability. The CCEB Strategic Plan transitions the CCEB Principals' guidance into goals and objectives that provide a foundation for combined interoperability. The CCEB Management Plan translates these goals and objectives into guidance for the Information Assurance (IA) Working Group's (and other CCEB working group's) detailed Plans of Work. The CCEB goals include:

(1) To develop and enhance combined Command, Control, Communications, Computers and Intelligence (C^4I) interoperability,

(2) To provide effective and interoperable communications and information services by influencing the implementation and future development of voice, data and video capabilities, and

(3) To enable an operational Combined Wide Area Network (CWAN);

b. **CCEB Information Assurance (IA) Working Group (WG).** This working group is responsible for the development of Allied IA policy and guidance for ratification by the nations, including the drafting of relevant ACPs. The IA WG will comprise representation from member CCEB nations to address IA interoperability issues as they arise. A single 'Lead delegate' will be nominated from within the Ministry/Department of Defence supported, as appropriate, by other specialists such as their national security authorities;

c. **Multinational Security Accreditation Board (MSAB):** The MSAB exists to facilitate and endorse the accreditation of all interconnected IS established between two or more of the Australia/Canada/New Zealand/United Kingdom/United States (AUSCANNZUKUS) nations and the North Atlantic Treaty Organisation (NATO). The principal role of the MSAB is to coordinate inputs from national accreditation agencies and issues a Coalition Accreditation Endorsement Certificate (CAEC) once all national approvals have been received and correlated. Uniquely, the MSAB is the security accreditation mechanism which provides a process of due diligence to ensure a holistic approach to the security of coalition information systems. The Board will perform its roles for the entire life cycle of the accredited systems or networks; and

d. **International Computer Network Defence (CND) Coordination Working Group (ICCWG):** The ICCWG is established under the auspices of the 2002 Memorandum of Understanding (MOU) for IA and CND (Australia, Canada, New Zealand, United Kingdom, and United States as signatories) and is responsible for:

(1) Providing required information to the signatories of the MOU and the CCEB IA WG,

(2) Reviewing progress of activities and coordinating reports as required for submission to the MOU signatories,

(3) Resolving multilateral IA and CND issues,

(4) Reviewing CND-related amendments to the MOU and forwarding them to the Participants for approval, and

(5) Maintaining oversight of the security aspects of the MOU.

DEFINITIONS

106. Definitions and acronyms used within this document appear in the glossary (Glossary-1), with sources shown where known.

DOCUMENT MAINTENANCE

107. This document shall be subject to the normal CCEB staffing process for ACPs, but as a minimum the ACP is to be reviewed every second year or when required to ensure that it remains consistent with CCEB national policies and evolving technologies. Suggestions for amendments should be forwarded through normal channels to the CCEB Washington Staff (WS).

CHAPTER 2

PRINCIPLES

DEFINITION

201. The NATO definition of Information Assurance (IA) utilized by CCEB is:

> "Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection and reaction capabilities."

CONTEXT

202. IA is a key enabler to support Combined operations. IA is not only concerned with information that is under direct attack; IA is also concerned with protecting information and CIS from natural disaster and human error.

203. IA is intrinsically linked to network operations. IA, network management and information dissemination management are all functions integrated under the concept of network operations.

GENERAL POLICY STATEMENT

204. A balanced set of administrative, physical, personnel, procedural and InfoSec (to include Computer Security (COMPUSEC), Communications Security (COMSEC), Cryptograhic Security (CRYPTOSEC), Transmission Security (TRANSEC) and Network Security (NETSEC), and Emission Security (EMSEC) measures shall be identified and implemented to create a secure environment in which a CIS can operate. These measures, as determined through a Vulnerability and/or Threat Risk Assessment (TRA), shall be implemented commensurate with the classification and/or sensitivity levels of the information being handled, stored, processed or transmitted, and the system assets, to ensure that confidentiality, integrity, availability and accountability concerns are adequately addressed. These measures shall be established concurrently with the design and development of the CIS.

205. A security policy and associated security documentation must be produced by a project office or nominated body at the outset of a project. The documentation will be the responsibility of that project office and evolved and maintained by them during the life-cycle of the project. The security policy and security documentation is an integral part of the accreditation process for the project. Guidance for the creation of a Multinational Security Policy can be found at Annex D.

206. The overall goal of the IA policy is to ensure the appropriate safeguarding of all sensitive information and assets under combined control in the context of CIS, as well as to

ensure that information required for operational support is available to the warfighter. The objectives of this policy are to ensure that:

a. All sensitive information stored, processed, displayed or transmitted by combined CIS are safeguarded in a manner consistent with this publication and its subordinate publications,

b. All sensitive assets, information and CIS products having intrinsic value to combined operational and management functions are safeguarded in a manner consistent with this publication and its subordinate publications, and

c. The residual risk of compromise to sensitive information and assets is reduced to a level acceptable to the combined force.

INFORMATION ASSURANCE ASSUMPTIONS

207. The following are basic assumptions for IA:

a. Info is always at risk from natural, accidental and deliberate actions; and

b. It is not possible to ensure absolute protection of information.

INFORMATION ASSURANCE OBJECTIVES

208. The following are the objectives of IA:

a. To protect information used in and for operational processes;

b. To control access to information by ensuring appropriate clearances are obtained and need-to-know principles are applied;

c. To provide the appropriate degree of information protection as determined by the criticality and security classification of the information; and

d. To verify a consistent approach to the protection of information.

INFORMATION ASSURANCE PRINCIPLES

209. The following security principles will need to be considered:

a. **Assurance of Protection.** CIS handling sensitive information shall provide assurance that its security functionality will perform consistently as specified. Both automated and manual techniques shall be employed regularly to verify that all required security mechanisms and procedures are invoked and operating properly;

b. **Availability.** Any user of a CIS shall be responsible to ensure that no actions are taken which could degrade or compromise the required level of responsiveness of programs, services and information being provided by the CIS to support the stated operational or managerial requirements;

c. **Confidentiality.** Any user of a CIS shall be responsible, within the span of their control, to ensure that no actions are taken which could degrade or compromise the confidentiality levels of the programs, services and information handled by the system;

d. **Continuity of Protection.** The minimum security policies, requirements and mechanisms for a CIS shall not be degraded except where it may be necessary to temporarily support an immediate operational necessity which clearly outweighs the potential security risks involved. In such cases every effort shall be made to inform all the CCEB member national security authorities as a matter of utmost urgency;

e. **Controlled Access.** A person or any system component shall be granted access to only that sensitive information and those assets for which appropriate access authorisation(s) and established need-to-know have been approved. A person or any system component shall be granted access to only those CIS resources necessary to perform the assigned task(s) and only when such access will not lead to a breach of this or any other principle of IA. Controlled access is normally achieved via physical and procedural means;

f. **Integrity.** Any user of a CIS shall be responsible, within the span of their control, to ensure that no actions are taken which could degrade or compromise the required level of accuracy, completeness and dependability of the programs, services and information being handled by the CIS or its assets;

g. **Individual Accountability.** Any person who uses a CIS shall be responsible and accountable to follow recommended procedures and to take all reasonable steps to safeguard the information handled by that system and any sensitive assets involved. All CIS should provide a means by which users can be held individually accountable for their actions;

h. **Least Privilege.** A person or any system component shall be granted the most restrictive set of privileges needed for the performance of authorised tasks. Least privilege is normally achieved via technical means once access has been granted;

i. **Levels of Protection.** The physical and logical protection provided to a CIS must be commensurate with the sensitivity levels of the information and assets involved and must take into consideration the identified threats to and vulnerabilities of the CIS;

j. **Redundancy of Protection.** Redundant protective features and procedures shall be employed in the safeguarding of sensitive information handled by a CIS and any sensitive assets involved, unless implementation of such measures is not possible or has been determined to be unnecessary by a TRA;

k. **System Stability.** All elements and components of the CIS shall function in a cohesive, identifiable, predictable and reliable manner, so that malfunctions can be detected and reported within a predictable period of time; and

l. **Survivability.** The Organisation employing a CIS must be capable of providing for continuity of operations to meet minimum essential level of services.

INFORMATION ASSURANCE COMPONENTS

210. The components of IA consist of the following:

a. Risk Management;

b. Certification and Accreditation;

c. Secure Operation;

d. Verification Activities;

e. Security Architecture;

f. COMSEC, encompassing CRYPTOSEC, TRANSEC and NETSEC;

g. EMSEC;COMPUSEC;

h. CND;

i. Personnel Security;

j. Physical Security; and

k. An Alert, Warning and Response (AWR) regime.

IMPLEMENTATION CONSIDERATIONS

211. Each participating nation has its own set of information assurance policies, procedures and doctrine, which are recognized and accepted by approved bilateral agreements as being adequate for the protection of each others information when passed between nations.

212. The purpose of this publication is therefore not intended to supplant the existing IA regimes operated by the participants, but rather to act as an agreed upon baseline for implementation of IA measures in an Allied environment.

213. Most of the requirements identified within this document will therefore be achievable by applying the relevant nation(s)' policies, and this document therefore is intended to act as an *aide memoire* to system implementers and security staffs to ensure that all the concerns have been addressed; only in those limited cases where a specific Allied interpretation is required should this document, or related documents need to be quoted as the definitive Policy.

214. The following Chapters therefore summarize the high level controls expected to be achieved by each of the components enumerated above: a checklist (the Accreditation Reference Sheet and Evidence Statement) is provided at Annex C to allow a quick check to be made that the requirements are met for each affected project or system.

CHAPTER 3

RISK MANAGEMENT

OVERVIEW

301. Combined forces increasingly rely on interconnected CIS for command and control, and administration purposes.[1]

302. The management of the risk to a CIS is effected through a system security architecture comprising operational, procedural, physical, personnel and technical components, selected in the light of an assessment of the risks to the system, the definition of system security requirements and the analysis of optional security architecture solutions. The design of the security architecture is an integral part of the system design. The development of the security architecture and its maintenance throughout the life of the system is accomplished through the security risk management process.

POLICY

303. In order to ensure that adequate, cost-effective security is provided to CIS, there is a requirement for the orderly examination of sensitivities, threats, and vulnerabilities in order to determine the risk to any given CIS and what protective measures/safeguards are required. This process is known as risk assessment, and is the fundamental basis of risk management. The security risk management process is applicable to all new and in-service CIS within combined operations. New systems shall start applying the risk management process at the beginning of the planning stage. Risk management for in-service systems forms part of the configuration management process.

RISK MANAGEMENT PROCESS

304. The security risk management process is the process by which resources are planned, organized, directed and controlled to ensure the risk to national or combined CIS and the information they handle remains within acceptable bounds at optimal cost. The process enables the definition, implementation and life cycle management of the system security architecture. It is equally valid for small stand-alone systems as for large networked systems - the difference in application lies in the degree of system complexity and the extent of the security requirement. The security risk management process applies regardless of where system planning, implementation and operation are accomplished.

[1] Not all of the information processed, stored or transmitted by these systems would be classified in the national interest. Some of it may be personal (evaluations, medical reports) or financial (project cost projections, budgets) information that is sensitive and therefore warrants some form of protection against unauthorised disclosure, removal, destruction, interruption or modification.

305. The process involves the identification of the risk to any of the IA principles inherent in the system and the management decisions concerning the acceptable level to which it may be managed. It consists of the following:

a. Evaluation of the sensitivity of the assets planned for the system and the information to be processed on it,

b. Determination of the risk of injury to those assets taking into account system vulnerabilities and gaps in the coverage of safeguards, and the threats which can exploit them,

c. Formulation of appropriate countermeasures,

d. Identification, quantification and management acceptance of the residual risk, and,

e. Management of the system throughout its in-service life in such a way as to ensure that risks to the system remain at an acceptable level.

306. Risk has two components: threat and impact. Both elements must be present for a risk to exist:

a. **Threat** - the likelihood that the event will occur, and

b. **Impact** - the consequences or gravity of the damage incurred if the event occurs.

307. Risks exist in the technical, procedural, personnel and physical arenas. They might affect confidentiality, availability or integrity of systems. The language used to describe them will therefore vary, except that impact should always be expressed the same way. For an impact to have significance, it has to affect an operational or business activity. Impacts should therefore be expressed primarily in operational terms: for example, a compromise of intelligence data might cause critical exposure of intelligence sources, political embarrassment and critically undermine the execution of operations. The impact of an environmental security problem might be expressed partly in terms of the replacement cost of a building or a set of equipment.

308. The operational impact from any one realized risk can change, depending on how long the interruption lasts. For example, if a key logistics system is unavailable for 24 hours, the result might be minor delays in the logistics chain. After 24 hours, operations might begin to be affected as critical stores can no longer be tracked or accounted for. After 48 hours, the operation might suffer severe delays as supplies fail to arrive, forcing the alteration or amendment of critical elements of operations. Where time is a critical factor in identifying impact, it should be acknowledged in the risk management documents.

309. In summary, risk management is the process of assessing risks and making sensible, accountable decisions about the handling of those risks. Once a risk has been identified, there are four basic ways of dealing with it:

a. **Tolerate** - acknowledge liability for the costs if the risk should be realized,

b. **Terminate** - abandon the activity or function which causes the risk,

c. **Transfer** - make it another agency's responsibility, e.g., an outsourcing partner or an insurance company, and

d. **Treat** - implement counter-measures to limit the likelihood and/or impact of the risk.

METHODOLOGY

310. Rather than developing a unique common methodology for risk management, national standards will be adopted for risk management in combined operations. This approach facilitates the nations' compliance with standards, and promotes enforcement of standards. For combined systems, the relevant Designated Approval Authority(s) (DAA) will make the decision regarding what constitutes an acceptable risk.

COUNTER-MEASURES

311. Those risks that cannot be accepted, transferred or avoided must be reduced by counter-measures. There are many types of counter-measure, which operate in one of the following arenas:

a. **Physical** (e.g., a perimeter fence),

b. **Procedural** (e.g., having an authorisation form signed by an appropriate person before a new user account is set up),

c. **Personnel** (e.g., security clearances required for system administrators and users, user training), and

d. **Technical** (e.g., use of an evaluated password mechanism).

312. Counter-measures are an actual cost, set against the potentially greater cost of the realized risk. That actual cost might be financial (e.g., the purchase, maintenance and licensing cost of a software package, or the personnel costs of an increased security force) or operational (e.g., slowing down information exchange between combatants by imposing a 'second authorised signature' rule for information release). The costs must be identified and recorded if properly informed risk management decisions are to be made.

CHAPTER 4

CERTIFICATION AND ACCREDITATION

OVERVIEW

401. In order to ensure all CIS meet certain IA standards, a process must be in place to verify that the implemented safeguards are adequate and operating properly. CCEB nations all have existing processes for the "certification and accreditation" of CIS. The challenge is to extend these processes to ensure that Coalition CIS are similarly certified and accredited to the satisfaction of the appropriate national accrediting authorities.

a. **Certification.** Confirms compliance of the security requirements with accepted standards of the proposed and implemented solution and provides the relevant accreditation authority the objective evidence required to make an informed decision confirming that the CIS adequately caters for the identified IA requirements and minimizes the residual risk to an acceptable level.

b. **Accreditation.** Accreditation is the official management authorisation to operate a CIS or network with a given set of constraints or operating parameters (e.g., period of time, security mode of operation, security classification level – as detailed in Annex A). It can take the form of formal Accreditation, an interim accreditation, or a waiver. A minimum expected set of deliverables (detailed in Annex C) is required to reach the point at which this accreditation decision can be made with the proper knowledge.

MULTINATIONAL SECURITY ACCREDITATION BOARD (MSAB) ENDORSEMENT

402. MSAB is the endorsement authority for CCEB CIS. The following text describes the purpose, role and responsibilities of the MSAB.

MSAB PURPOSE, ROLE AND RESPONSIBILITIES

403. Purpose. The MSAB exists to facilitate and endorse the accreditation of all interconnected CIS established between two or more of the AUSCANNZUKUS nations and NATO. Additional coalition nations will be considered when sponsored by AUSCANNZUKUS nations and NATO;

404. Role. The MSAB coordinates inputs from national accreditation agencies for networks that interconnect. The MSAB Chairperson issues a CAEC once all participating national approvals have been received. Uniquely, the MSAB is the security accreditation mechanism which provides a process of due diligence to ensure a holistic approach to the security of coalition information systems. The Board will perform its roles for the entire life cycle of the accredited systems or networks; and

405. Responsibilities. The MSAB members are responsible for:

a. Identifying the national POC on coalition accreditation issues,

b. Providing advice relating to the MSAB processes to the coalition project office, national project offices and the National Accreditation Authority (NAA),

c. Reviewing their national security accreditations to protect multi-national interests,

d. Providing a National Accreditation Endorsement Certificate (NAEC) to the Project Office /Coalition Project Office/ MSAB Chair and copied to MSAB members for systems requiring endorsement,

e. Ensuring that their NAA accredits the system of any guest nation they sponsor, and

f. Issuing a CAEC to the Project Office once all nations have issued NAEC.

NATIONAL MAPPING

406. The following table summarises variations in terminology between the CCEB participants, and provides details of the MSAB signatories and national lead authority for any clarification required on this topic.

	AUS	**CAN**	**NZ**	**UK**	**US**
Terminology	Accreditation	Accreditation	Accreditation	Accreditation	APPROVAL TO OPERATE
MSAB Signatory	CIO	D IM Secur	CIO	DGS&S	Joint Staff J6
Lead Authority	CIOG DISSP	D IM Secur	DJCIS	DGS&S DSSO	Joint Staff J65C

407. The Members' representation on the Board will either be a representative of the participant's Security Accreditation Authority, or a representative who is authorised to express the consolidated views of all relevant Authorities where more than one of a participant's Security Accreditation Authorities are affected by the matters under consideration by the Board.

408. The addition of Members to the MSAB is subject to unanimous agreement.

409. All projects, systems or networks authorities requesting endorsement by the MSAB may be required to send a representative to supply the MSAB with relevant information.

REPORTING

410. MSAB members are responsible to their national authorities for reporting the activities of the board.

ACCREDITATION PROCESS

411. In accordance with existing National Policies and agreements, the interconnection of national networks and services with those of another nation may only occur after both networks have been accredited by each NAA and the MSAB have endorsed the connection.

412. Each NAA accredits their component of the interconnecting system and notifies their National MSAB representative of the accreditation. The National MSAB representative then issues a NAEC to the MSAB Chairperson. After receiving all NAECs for the interconnection, the MSAB chairperson issues a CAEC to each participating nation and appropriate national MSAB representatives.

413. Any significant changes to an accredited national network that forms part of a coalition network may require accreditation by the relevant NAA, subject to national policy. If this is the case, then the national MSAB representative must issue an updated NAEC and the MSAB chair will need to issue a subsequent CAEC for the coalition network.

414. In respect of multi-national systems, such as the GRIFFIN 5-eyes and MIC GRIFFIN domain, a coordinated multi-national threat assessment must be produced covering the multi-national domain of the system to be accredited.

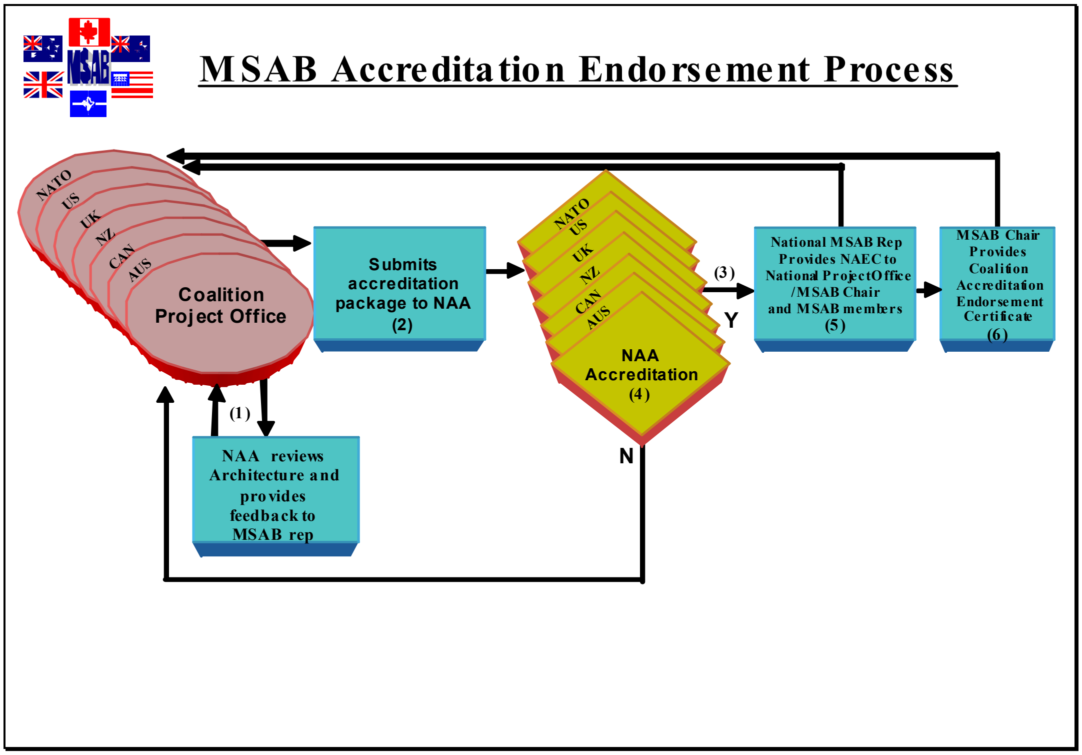
MSAB Accreditation Endorsement Process
MSAB
NATO
US
UK
NZ
CAN
AUS
Coalition Project Office
Submits accreditation package to NAA (2)
(1)
NAA reviews Architecture and provides feedback to MSAB rep
NATO
US
UK
NZ
CAN
AUS
NAA Accreditation (4)
(3)
Y
N
National MSAB Rep Provides NAEC to National ProjectOffice /MSAB Chair and MSAB members (5)
MSAB Chair Provides Coalition Accreditation Endorsement Certificate (6)

Figure 4-1: The Accreditation Process

1. All projects, systems or networks requesting endorsement of the MSAB (inclusive of guest nation activities) may be required to brief the MSAB during the development process.

2. National project office submits accreditation package to NAA for approval. When connecting for testing purposes only, then NAA can approve, but national MSAB representative is to be notified.

3. NAA advised the national MSAB representative when the national system is accredited.

4. The NAA is responsible for accrediting any guest nation.

5. The MSAB national representative is responsible for providing the NAEC of any guest nation they sponsor.

6. MSAB chair provides CAEC when all nations connecting to network or systems are accredited.

ISSUE RESOLUTION

415. If there is any confusion or disagreements with the status of the accreditation of any component of a coalition system then issue is to be forwarded to the MSAB Chairperson. The MSAB Chairperson will use any of the available MSAB resources to resolve the issue.

GENERIC REQUIREMENTS

416. Interconnection Gateways: All equipment used to facilitate an interconnection between participating national networks or security domains should be certified to the appropriate level via the Common Criteria process. If this is unachievable, then a risk managed solution will need to be determined. As all participating Nations/Organisations will need to accept the risk, the MSAB will provide the mechanism for coordinating the actions through each national MSAB representative. Any requests for this action should be facilitated through the relevant national MSAB representative.

CHAPTER 5

SECURE OPERATION

OVERVIEW

501. Not only does a CIS have to be implemented in a secure manner, but the manner and environment in which it is operated also needs to remain appropriately secure. The responsibility for maintaining this posture rests jointly with a number of interlocking functions:

a. System Operating Authorities (SOA),

b. Security Staffs:

(a) ISSOs, those responsible for the security of the CIS which can encompass but is not limited to the Intrusion Detection element of the Defensive Information Operations (DIO) mission, and

(b) Those charged with maintaining the security of the environment, such as Physical and Personnel aspects;

c. End Users.

502. These aspects are covered in a variety of security instructions.

NATIONAL MAPPING

503. The following table summarises variations in terminology between the CCEB participants, and provides details of the national lead authority for any clarification required on this topic.

	AUS	**CAN**	**NZ**	**UK**	**US**
Terminology		OpSec		SyOPs	SECOPS
Lead Authority	CIOG DISSP	D IM Secur	DJCIS	DGS&S DSSO	Joint Staff J65C

MEASURES REQUIRED

504. Although Secure Operation in an Allied and Coalition context will be handled in line with existing national procedures, the following specific topics should be considered:

a. **Accounting and Safeguarding.** There may be associated information and material that must be handled, stored and transmitted in a particular way due to its classification/sensitivity, and those assets will need to be identified;

b. **Back Up Measures.** File system backups not only provide protection in the event of hardware failure or accidental deletions, but they also protect against unauthorised changes made by an intruder;

c. **Banners.** Part of the privacy issue centres around an individual's expectations of privacy when using a system. It is essential that individuals using an official CIS be conditioned not to have an expectation of privacy when using these systems;

d. **Business Continuity/Disaster Recovery.** Provision must be made for restoring operational capability in the event of an incident or disaster;

e. **Computer Network Defence.** Techniques, procedures and agreements with respect to CND must be provided as discussed below;

f. **Configuration Management.** Effective management of residual risk requires continuous evaluation of threats the system is exposed to. Identifying and managing the vulnerabilities and capabilities of the system and the environment will minimize the risk. Any changes to a CIS must be controlled, tracked and managed to ensure that additional risks that may be introduced by these changes are reviewed and either mitigated or deemed acceptable accordingly;

g. **Emergency Situations.** Actions to be taken in the event of a bomb threat, fire, or any other emergency situation;

h. **Exercises.** Exercises may be conducted to determine if the procedures defined are adequate for the threat to be countered;

i. **Incident Handling.** While every reasonable precaution can be taken to prevent the unauthorised disclosure, loss, manipulation, or denial of access to classified or sensitive information, there will be occasions when information security incidents will occur, and the Reporting and Response regime at Chapter 14 will be required;

j. **Media Security.** Including maintaining an inventory of classified media, proper marking, and rules governing Disposal and Reuse;

k. **Methods of Destruction.** Destruction of media should be accomplished in the most practical manner, and considering operational constraints (emergency burning in an incinerator or using flammable substances at hand, sinking in waters that would make salvage impossible); and

l. **Over-Riding Of Security Controls.** In some instances, it may be necessary to over-ride some security features; the procedure on how to over-ride the feature, and documenting the occurrence should be documented.

COMPUTER NETWORK DEFENCE (CND)

505. All CIS which will be used throughout CCEB nations will require a CND capability, which is normally implemented using a range of accredited security devices, including Intrusion Detection Equipment (IDS), manned by specially trained personnel. However, it is important to note that technical detection and response is only one element of CND, which is also reliant on effective reporting alert, warning and response mechanisms and involves all personnel who use, manage and maintain CIS.

506. The open and rapid exchange of IA and CND information between allies using connected systems is an essential element of the defensive Information Operations (IO) process, and falls within the purview of the ICCWG.

CHAPTER 6

VERIFICATION ACTIVITIES

OVERVIEW

601. Even with the implementation of security safeguards, which will be based on the results of a threat, vulnerability and risk analysis, a certain amount of residual vulnerability will always remain. If undetected or uncorrected, adversaries could exploit these vulnerabilities at critical times of their choosing, to the detriment of CCEB member nation operations.

602. The concept of shared risk implies that there is a corresponding requirement to share responsibility for the protection of combined CIS. Protection of these systems will require both passive and active measures, including verification services in support of coalition operations, and specifically in support of the combined CIS.

NATIONAL MAPPING

603. The following table provides details of the national lead authority for any clarification required on this topic.

	AUS	CAN	NZ	UK	US
Lead Authority	CIOG DISSP	D IM Secur	DJCIS	Dir Business Resilience DSSA	Joint Staff J65C

VULNERABILITY ANALYSIS (VA)

604. Vulnerability analysis is a systematic examination of a CIS or Organisation to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

605. Vulnerability analysis will assist in overall security management of combined CIS by:

a. Identifying and analyzing combined CIS vulnerabilities,

b. Advising combined security officials on compliance with agreed combined standards for CIS security, and

c. Providing advice and support for the reduction or elimination of these vulnerabilities, seeking to prevent or minimize damage due to loss or compromise of combined CIS services.

VA ACTIVITY LEVELS

606. Within the CCEB context, VA activities are categorised into four incremental levels of effort:

a. **VA Level 1 – Primary Investigation.** Identify and validate all system and connected network elements, analyse topology and locate obvious vulnerabilities and/or initial entry points;

b. **VA Level 2 - Vulnerability Sweep.** Exploit vulnerabilities discovered during VA Level 1, gaining basic access to accounts, and attempt to crack passwords;

c. **VA Level 3 - Security Sweep.** Exploit vulnerabilities for greater access, exploit trusted relationships, exploit new vulnerabilities; and

d. **VA Level 4 – Stress Testing**. Test the system to ensure resilience to denial of service (DoS) attacks. VA4 must be authorised by the Security Authority (SA), in consultation with the operational and business sponsors, and will normally only be appropriate for Mission Critical systems.

ACTIVE VULNERABILITY ASSESSMENT

607. In addition to vulnerability analysis to identify and correct CIS vulnerabilities, there is also a requirement to provide an independent capability to assess vulnerabilities and improve defences.

608. The main aim of the assessment is to help system administrators and ISSOs ensure the security of their networks. It may involve penetration testing and instruction of relevant staff on how to recognise CIS events and determine the appropriate actions required to respond to those events. To ensure the validity of these assessments, it may be desirable to exclude system administrators and ISSOs from prior knowledge of the exercise.

609. Each nation will conduct the assessment on their own systems in accordance with their own national policies and procedures and undertake to remediate any detected vulnerabilities as soon as practicable.

610. In the multinational environment, assessments may be conducted at the request of the operational authority for the multinational environment. Policies and procedures with respect to VA in multinational environments will be delineated in the applicable System Security Policy (SSP).

VULNERABILITY ASSESSMENT

611. Vulnerability assessment shall not be limited to technical vulnerability analysis. Vulnerability assessment shall be part of an operational evaluation of a unit/formation and should include (but not be limited to):

a. Physical Security Survey,

b. Review of personnel security clearances and formal access privileges to ensure that they are consistent with requirements,

c. Review of local security policies, standards and procedures, contingency and response plans, etc., to ensure they are current, accurate and relevant,

d. Assessment of the unit/formation Operational Security posture,

e. Review of local security administration, and

f. Defensive nodal analysis.

612. Vulnerability assessment shall be part of the certification and accreditation process, every exercise and operation (as part of the force protection process); and/or conducted periodically as determined by the appropriate authority. It shall be conducted by the appropriate technical authority on a non-interference basis in co-ordination with the operational system owner and shall not involve the modification, manipulation, insertion, removal or destruction of existing information.

613. The information collected during vulnerability assessment may contain details of combined partner CIS vulnerabilities and will therefore be extremely sensitive or classified. Some of it will be national proprietary information. Unauthorised disclosure of this information could have grave consequences for combined security. Accordingly, all vulnerability assessment results shall be classified on the basis of:

a. The sensitivity of the data processed on the system,

b. The criticality of the system and information to Combined operations, and

c. The severity and potential impact of the vulnerability.

614. Noting the sensitivities associated with CIS vulnerabilities; provision shall be made for the removal of system or host specific details such as host name or host IP address from any reports. Any references to third parties shall also be removed. General findings will be provided for, but not be limited to, the following:

a. Statistical analysis,

b. Periodic reports by authorised combined entities, and

c. After action and Lessons Identified reports.

TELECOMMUNICATIONS SECURITY MONITORING

615. Telecommunications Security monitoring and analysis can be an integral part of an overall security programme. It provides a means to assess vulnerability resulting from unsecured communication and to evaluate how effectively relevant security policies and procedures are being implemented. It also indicates areas where changes, improvements and training are required to enhance the overall security posture.

616. Telecommunication in this sense is defined as:

a. Communication by wire, radio, optical, or other electromagnetic means, and

b. Any transmission, emission or reception of signs, signals, writing, images and sounds or intelligence of any nature by wire, radio, optical, or other electromagnetic system.

617. This definition specifically includes all forms of voice, data, facsimile, message and graphical interchange.

POLICY

618. Where surveillance of combined telecommunications is a required and approved military command function this will be undertaken by the coordination of national monitoring activities. Any monitoring performed for security reasons shall therefore be conducted in accordance with appropriate national laws.

TECHNICAL SECURITY INSPECTIONS

619. The mandate of a Technical Security Inspection (TSI) Team is to provide sweeps against surreptitious audio, video or electronic listening devices, and ongoing monitoring of secure or sensitive spaces and facilities. A TSI team can also provide recommendations to the operational authority on deficiencies in Secure Signal Intelligence (SIGINT) Areas (SSAs) or Sensitive Discussion Areas (SDAs), where discovered, and measure attenuation levels for speech privacy. Their role is purely defensive. They are normally tasked by arrangement through national authorities.

620. Areas such as SSAs (also known as Secure Compartmented Information Facilities (SCIFs)), SDAs, SA material holding areas, conference halls, and selected private residences shall be subject to periodic inspection as per national policy.

CHAPTER 7

SECURITY ARCHITECTURE

OVERVIEW

701. The CIS architectures of the CCEB member nations are highly interconnected and distributed computing environments. Users access and share various information holdings across CIS, regardless of where they happen to be when they need the information. This is a fundamental business and operational requirement, one that is accelerated by the rapid pace with which information technology is advancing. At the same time, it is this requirement for distribution and interconnection that makes the infrastructures inherently difficult to secure; there is a balance that must be achieved in making, on one hand, information widely available while, on the other hand, securing the information in accordance with national security policies.

702. The solution to this apparent incompatibility is a generic security architecture that is fully integrated into the overall CIS architecture, such that security services are, to the greatest extent possible, invisible to the user and continuously invoked. A security architecture is defined as "a system-specific set of complementary operational, procedural, and technical security measures selected and organized in a logical and effective manner to protect the confidentiality, integrity, and availability of system assets at a level determined through risk assessment and accepted by the system owner, as advised by the security authority".

703. In the combined environment, the balance between security and operational capability is more difficult, as nations remain responsible for maintaining the security of their respective CIS while extending the interconnections outside national boundaries.

POLICY

704. System specific security measures shall be commensurate with the confidentiality, integrity, availability, and accountability requirements of the system (identified through a TRA). They shall, to the greatest extent possible, be consistent with the existing approved security architecture. This will ensure the most effective and efficient use of common security mechanisms and components for the protection of combined CIS, including the employment of detection, containment, and recovery principles.

NATIONAL MAPPING

705. The following table provides details of the national lead authority for any clarification required on this topic.

	AUS	CAN	NZ	UK	US
Lead Authority	CIOG DISSP	D IM Secur	DJCIS	MOD CIO	Joint Staff J65C

INTERCONNECTION SCENARIOS

706. In addition to bilateral or multilateral connections using dedicated infrastructures, a growing number of coalition interconnections are achieved using shared infrastructures.

707. In the context of multinational communications and information systems, the concept of three fundamental types of systems has evolved. These systems have their own security policies and accreditation requirements:

a. **National Affiliated System (NAS).** System(s) under a nation's control connected to a Shared Information System, but not included in it, that process, store or transmit national information,

b. **Combined Communications and Information System(s) (Combined CIS).** System(s), including interconnecting networks and supporting infrastructure elements, which process, store and transmit shared information, and

c. **Shared Communications and Information System(s) (Shared CIS).** System(s), including interconnecting networks and supporting infrastructure elements, which process, store and transmit shared information; and over which participating member nations share responsibility for its operation.

CHAPTER 8

COMMUNICATIONS SECURITY

OVERVIEW

801. COMSEC encompasses CRYPTOSEC, TRANSEC and NETSEC.

PRINCIPLE

802. When being passed outside of secure areas, all classified information is to be protected by either:

a. Government approved cryptography; or

b. A protected distribution system.

CRYPTOGRAPHIC SECURITY (CRYPTOSEC)

803. CRYPTOSEC can be provided through hardware or software means, and cryptographic methods can be used to achieve traditional confidentiality, but they can also be used to achieve integrity, availability, and accountability (access control, identification and authentication, non-repudiation).

NATIONAL MAPPING

804. The following table provides details of the national lead authority for any clarification required on this topic.

	AUS	CAN	NZ	UK	US
Lead Authority	DSD CIOG	D IM Secur	DJCIS	DGS&S InfoSy(Tech)	NSA IAD

805. Appropriate and approved CRYPTOSEC measures shall be used to safeguard confidentiality, integrity, availability, and/or accountability of all classified and extremely sensitive information stored or transmitted by electronic means. As well, where justified by a TRA, electronic information of a low-sensitive or particularly sensitive nature shall be protected by approved cryptographic methods.

806. CRYPTOSEC relies on two basic building blocks:

a. **Crypto Devices**. Used to provide data confidentiality and integrity while being transmitted through hostile environments, and managed in accordance with current National and Allied publications, and

b. **Keying Material**. Keying material for Crypto Devices, provided from National or Allied sources and handled in accordance with current National and Allied publications.

807. CRYPTOSEC activities in an Allied and Coalition context will be handled in line with existing national procedures.

TRANSMISSION SECURITY (TRANSEC)

808. TRANSEC is that component of information security that results from the application of measures designed to protect transmissions from interception and exploitation by means other than crypto analysis.

809. Traffic flow analysis is a form of threat against communications from which intelligence can be gained, despite the use of encryption on the content of the traffic. It should be considered when designing and fielding a CIS that uses an uncontrolled transmission medium (e.g., free space or public carrier).

TRANSEC SCOPE

810. Telecommunication in this sense is defined as:

a. Communication by wire, radio, optical, or other electromagnetic means; and

b. Any transmission, emission or reception of signs, signals, writing, images and sounds or intelligence of any nature by wire, radio, optical, or other electromagnetic system.

TRANSEC MEASURES

811. TRANSEC activities in an Allied and Coalition context will be handled in line with existing national procedures.

812. TRANSEC measures can be divided into two main categories: technical, and operational/procedural. Examples of technical measures are the use of Limited Probability of Intercept (LPI) techniques such as frequency hopping or spread spectrum, and the use of directional antennas. Examples of procedural measures include the employment of radio silence, emission control (EMCON), or MINIMIZE.

813. Whenever justified by a TRA, appropriate procedural or technical transmission security measures shall be implemented for the transmission of classified or otherwise sensitive information. The implementation of these TRANSEC measures will be independent of any CRYPTOSEC measures that might be required. Detailed direction regarding TRANSEC will be contained in the specific security requirements identified for the combined CIS in question. If technical measures are employed, interoperability must be considered.

NETWORK SECURITY (NETSEC)

814. There is an increasing tendency for CIS and networks to be interconnected, as a means of communication and sharing information. There are additional security concerns that arise when systems are interconnected, whether they are local area networks (LANs), metropolitan area networks (MANs) or wide area networks (WANs). Network security protects networks and their services from unauthorised modification, destruction, or disclosure, and provides assurance that the network performs its critical functions correctly.

NETSEC MEASURES

815. NETSEC activities in an Allied and Coalition context will be handled in line with existing national procedures, considering the following aspects:

a. **PSTN Communications.** Communications using the PSTN should be protected using an approved authentication device, to ensure that all users accessing the network are authenticated, and to prevent intruders from breaking into the system;

b. **Communicating Classified Information Over the PSTN**. Where the PSTN is to be used to transmit classified information, an approved encryption device and voice authentication procedures should be used to protect the transmission. The same voice authentication procedures should be followed for secure fax;

c. **Communications Servers**. Users should normally only use comms servers for communicating externally, and should not introduce any modems to their workstations, as this could allow back-end access to the network;

d. **Extent of Network Connections**. The Sponsor(s)/Owner(s) are to obtain details of the extent of all connections, for inclusion in the system security policies and inform the Network Managers of onward connected systems;

e. **Degree of Access**. The Sponsor(s)/Owner(s) are to establish a written understanding of the degree of access that users of the system will have to other connected systems;

f. **Access Control**. The Sponsor(s)/Owner(s) are to determine the access controls that will be used to control users of the system when accessing the other connected systems;

g. **Network Management Disputes**. The Sponsor(s)/Owner(s) are to establish a process by which dispute over network management issues can be resolved or be taken to a higher authority for resolution; and

h. **Information Aggregation**. The Sponsor(s)/Owner(s) are to recommend to the national Defence Security Authority, the information aggregation situations that may require a security classification higher than that of the individual information items to which access is allowed on the network.

INTEROPERABILITY CONCERNS

816. The following concerns regarding interoperability should be considered when implementing a combined CIS:

a. Just as a network needs to be managed from a performance point of view, there should also be some mechanism (or agency) to cater for the effective management of NETSEC measures (including configuration management, security management, key management, and access control);

b. While cryptography can effectively deal with confidentiality and integrity in a network, other measures are necessary to deal with availability issues (fault tolerance, recovery procedures and redundancy); and

c. The interconnections of a CIS to other systems (e.g., within a Service, or with allies) must be identified and it must be confirmed that the implementation of the interconnections satisfies the needs for adequate protection of sensitive information on the system. The adequate protection of sensitive information on the system is affected by the potential sharing of sensitive information with other members of the organisation and with other governments and organisations.

CHAPTER 9

CCEB GUIDANCE ON SECURITY LABELLING

INTRODUCTION

901. The CCEB nations are introducing national messaging systems and messaging gateways that will provide significant functional enhancements to Military Messaging (MM) and other information services. In order to achieve international interoperability there is a requirement for Security Labelling guidance that provides as much commonality as possible in order to minimize complicated mapping at national boundaries and enhance ease of use.

902. At CCEB Collocated Meeting No 9, the Messaging Policy and Procedures Tiger Team (MPPTT) made a number of recommendations that sought to resolve the security labelling issues that affect the CCEB nation's ability to exchange information through messaging. This Chapter is an expansion of the MPPTT work.

AIM

903. The aim of this Chapter is to provide CCEB Security Labelling guidance in sufficient detail to enable nations to configure their messaging systems and/or messaging gateways in order that they deliver information appropriately and in accordance with information handling agreements between nations.

SCOPE

904. This Chapter seeks to define elements of the Security Label to assist both system users and technical implementers by providing common understanding so that the application of labels within messaging systems is as clear and unequivocal as possible. Whilst this Chapter concentrates on the Security Labelling issues for MM it should be applied across all types and grades of messaging and information services where and if applicable.

SECURITY LABEL ELEMENTS

905. There are a number of elements (or fields) that make up the Security Label. The following paragraphs describe what they are, identify issues associated with them and explain how they should be handled.

POLICY IDENTIFIER.

906. Due to the increase of coalition based operations the use of a Policy Identifier is important in order to clearly identify the owner or originator of the information. There are also broader implications for the user of Policy Identifiers since many of the CCEB nations have standing responsibilities in International Defence Organisations (IDOs) (i.e. NATO, WEU). (e.g. NZL CONFIDENTIAL, NATO RESTRICTED)

907. When, and if possible, countries that do not mandate the use of policy identifiers on their messaging systems or are not able to allocate one, the appropriate national policy identifier should be applied at the originating national boundary.

CLASSIFICATION.

908. The Classification is a grading given to information or material to show the degree of damage that could result from its unauthorised disclosure and the standard of protection to be given to it. Whilst there is general agreement and understanding within the international community on the meaning of TOP SECRET, SECRET, CONFIDENTIAL and UNCLASSIFIED[2], a number of nations do not use the term RESTRICTED. Equivalences and subsequent mapping should be in accordance with the appropriate bi-lateral agreement. It should be noted that there may be occasions when, due to the differences in bilateral agreements between nations, a message that has been forwarded to a third nation may bear a higher classification than the one assigned by the originator. This is commonly known as 'label creep'. e.g.

a. AUS sends a message with a Classification of RESTRICTED to the USA and UK. The bilateral agreement between AUS and the USA states that the USA will treat the message as CONFIDENTIAL.

b. The USA replies to the message, copying UK. Both AUS and the UK receive the reply with a Classification of CONFIDENTIAL.

909. Where possible, it is desirable that the original label is retained in order to clearly show the originators intent and ensure that the recipient knows how the information is to be handled in accordance with the applicable bilateral agreement. This only applies where differences in bilateral agreements may change the allocated classification (e.g. the originators label 'CAN PROTECTED A' could be displayed as 'CAN PROTECTED A (RESTRICTED)' when delivered to a UK recipient.)

CATEGORIES.

910. **Descriptors**. Whilst the CCEB uses descriptors, some of which are common to all nations, they are not intended for use in international communications and will not be passed through MM gateways.

911. **Codewords**. Coordination is required between CCEB nations if a Codeword is to be used internationally as part of the Security Label to ensure it is managed appropriately. When, and if applicable, nations should include a field within the security label that is capable of supporting Codewords. This will enable users of messaging systems to exchange information that contain codewords common to nations. Codewords will have specific Security Enforcing Functions (SEFs) applied to them in order that the information contained in a message is distributed and handled appropriately.

[2] The marking or description given to information which is not protectively marked.

912. **Caveats**. Caveats are used by an originator to limit the release of information to specific countries or IDOs. There are two caveats that are widely used by CCEB nations to do this: RELEASABLE TO and EYES ONLY. The definition of these terms is equivalent and national policy together with individual bi-lateral agreements on information handling should be applied.

913. When sending a message outside a national boundary, originators of a MM will be required to choose one of 2 internationally accepted caveats (RELEASABLE TO or EYES ONLY). For example:

a. If a UK originator wishes to send a CONFIDENTIAL message to the USA the minimum permissible security label would be:

(a) UK CONFIDENTIAL UK/USA EYES ONLY.

b. An originator, for example USA, sending a message to NZL may wish to indicate that its content is releasable to other nations.

(a) USA SECRET RELEASABLE TO USA /AUS/CAN/NZL/UK/

c. An originator sending a message to NATO may wish to indicate that its content may be released to the wider NATO community and other non NATO nations.

(a) UK RESTRICTED RELEASABLE TO AUS/NATO/NZL

COUNTRY CODES.

914. With the exception of the UK[3] all other country codes will be displayed in their 3 letter form in accordance with ISO 3166.

INTERNATIONAL DEFENCE ORGANISATIONS.

915. IDOs can be used within the Caveat element of the security label. Whilst the membership of IDOs is widely known and relatively stable it is important that both originators and recipients are aware of the membership of an IDO when assigning it to a caveat.

916. The same considerations apply to CJTFs and Coalitions. At this time the complexities in managing these makes it difficult to safely use them within messaging systems. Further investigation of how best to employ them is required.

LABEL STRUCTURE.

917. **Human Readable**. The human readable structure of the Security Label is as follows:

[3] UK will remain in use until the UK Government security policy mandates otherwise.

[Policy Identifier] [Classification] Categories in order of use [Descriptor], [Codeword] [Caveats]

e.g.

UK RESTRICTED AUS/CAN/NZL/UK/USA EYES ONLY

NZL CONFIDENTIAL RELEASABLE TO AUS/CAN/NZL/UK/USA

918. **Machine Readable**. The machine readable structure of the Security Label should be in accordance with the Internet Engineering Task Force (IETF), Request For Comments 2634 (RFC2634) and NATO AC/322-D(2004)0021.

CONCLUSION

919. With the proliferation of automated information systems it becomes increasingly important in the complex world of coalition operations that we strive to achieve commonality in security labelling. A robust guidance on the use of Security Labelling ensures the characteristics of the grade and type of messaging and information services with which they are associated are maintained to prevent the inadvertent release of information.

CHAPTER 10

EMISSION SECURITY

OVERVIEW

1001. EMSEC is the protection resulting from all measures that deny unauthorised persons information that can be derived from the interception and analysis of compromising emanations from CIS.

1002. TEMPEST refers to the study and control of spurious electronic signals emitted from electronic equipment. It is a codeword, not an acronym. Stringent standards have been developed and rigidly applied in order to test the varying levels of compliance with the TEMPEST standards. Testing is only authorised to be performed by certified TEMPEST professionals.

NATIONAL MAPPING

1003. The following table summarises variations in terminology between the CCEB participants, and provides details of the national lead authority for any clarification required on this topic.

	AUS	CAN	NZ	UK	US
Terminology	TEMPEST	EMSEC		RADSEC	EMSEC
Lead Authority	DSA DISSP	D IM Secur	DJCIS	DGS&S InfoSy(Tech)	Joint Staff J65C

MEASURES REQUIRED

1004. All establishments, ships, submarines, aircraft and vehicles, as well as industry under contract, shall protect sensitive information against compromising emanations. EMSEC requirements shall be identified for electronic equipment processing, storing or transmitting classified or otherwise sensitive information, based on the results of the TRA process. Testing of the effectiveness of EMSEC measures shall also be conducted.

1005. EMSEC activities in an Allied and Coalition context should be handled in line with existing national procedures, considering the following aspects:

a. **EMSEC Threat Assessment.** An EMSEC threat assessment is to be undertaken for all Allied information systems, in accordance with national policy,

b. **Installation Standards.** Cables carrying unencrypted red (classified) information shall be physically isolated from cables carrying black (unclassified) information to prevent signal coupling between the lines. Installation of equipments shall consider grounding and bonding issues, and the filtering or isolation of circuits, and

c. **Facility Emission Security (EMSEC) Zoning**. To maintain the integrity of the EMSEC zoning status of a facility, no user shall tamper with or move any TEMPEST-certified equipment unless specifically directed by the ISSO, and no one shall tamper with any TEMPEST shield, including drilling holes, cutting or putting dents in the shield. Persons wishing to submit work orders for work within or immediately adjacent to a shielded enclosure shall seek the guidance of the ISSO. No one shall move or tamper with the cable distribution system.

CHAPTER 11

COMPUTER SECURITY

OVERVIEW

1101. COMPUSEC is the protection of computing systems against threats to confidentiality, integrity, availability, and accountability. It must address the threats to electronic transactions and files. The context of computer security is always changing, due to rapidly changing technology, decentralization, networking, privacy issues, and the potential for fraud and abuse.

NATIONAL MAPPING

1102. The following table provides details of the national lead authority for any clarification required on this topic.

	AUS	CAN	NZ	UK	US
Lead Authority	CIOG DISSP	D IM Secur	DJCIS	DGS&S InfoSy(Tech)	Joint Staff J65C

COMPUSEC MEASURES

1103. COMPUSEC measures (hardware and software security features) shall be required to implement fundamental IA principles (e.g., access control, audit, need-to-know separation):

a. **Hardware Security.** Examples are smart cards and biometric devices. Supplementary requirements for systems with sensitive information or assets will be identified in the TRA, and

b. **Software Security.** Examples are access control lists, encryption, trusted operating systems, and malicious code filters. Where information of differing sensitivities is being processed or stored and the users do not share a common need-to-know, particular attention shall be given to the manner in which the operating system and access control system are implemented.

1104. Whenever justified by a TRA, appropriate procedural or technical computer security measures shall be implemented for the automated processing of classified or otherwise sensitive information. The requirement for these COMPUSEC measures will be derived from a TRA. Detailed direction regarding COMPUSEC is contained in national documentation, but as a minimum the following aspects should be considered for Allied CIS:

a. **Identification and Authentication - Passwords.** Default passwords must never be assigned to accounts. New passwords, that cannot easily be guessed, must be created for each new user. These must be changed regularly especially when users with high access rights leave,

b. **Dial-In/Out Accounts.** Users should be briefed on the security problems inherent in providing dial-in access. Such connections should be used only on a strictly mission-critical basis and when no other type of connections are available,

c. **Privileged Accounts.** Access to privileged user accounts should be monitored, and only used when needed; unless the privileges are needed all the time, the user should be encouraged to have a 2nd, standard account for routine use,

d. **Operating System Software Configuration.** Users shall not modify the operating system software configuration without the consent of the ISSO or the Information Systems (IS) Manager,

e. **Detection and Surveillance - Audit Records.** All security relevant-events, as defined by national policy, shall be recorded in audit records,

f. **Remote Diagnostics.** Remote diagnostics should not normally be provided for Classified CIS,

g. **Malicious Software.** A malicious software strategy shall be maintained. All data shall be checked on export. The requirements for handling malicious software, as laid down at Chapter 14, should be known by all users,

h. **Import of Information.** The import of all information into an IT system from any source, either by media or a network connection to an external system, is to be approved in accordance with operating procedures. It is also to be legally acquired and used in accordance with the licence agreement,

i. **Handling and Marking of Electronic Storage Media.** All types of removable electronic storage media are to be labelled, handled, accounted for, de-classified or re-classified, and disposed of, in accordance with their security classification,

j. **On-site Maintenance of Classified Hardware and Media.** If classified assets of a Defence information system are maintained on-site, the maintainer is to either hold a security authorisation and/or clearance at the appropriate level, or be escorted by someone who is authorised and/or cleared, and

k. **Off-Site Repair of Classified Hardware and Media.** If classified assets of an information system are repaired off-site, the removal and repair of the media is to be in accordance with (i) above.

TRUSTED COMPUTING BASE

1105. One method of providing COMPUSEC is through the use of a Trusted Computing Base (TCB), which is the totality of components that together enforce a unified security policy over a product or system. CCEB nations have in the past employed different standards for evaluating the assurance of TCBs (TCSEC, ITSEC, CTCPEC), however, the Common Criteria has been developed and has been endorsed by several nation's national security authorities (Australia, Canada, Finland, France, Germany, Greece, Italy, Netherlands, Norway, Spain, the United Kingdom, and the United States).

CWAN ASPECTS

1106. In a CWAN environment, it is essential that the interoperability implications of any COMPUSEC measures applied in NAS and shared CIS be considered.

CHAPTER 12

PERSONNEL SECURITY

OVERVIEW

1201. There is a risk that any person who enters a facility containing CIS equipment may interfere with or damage the equipment, or see classified or sensitive information being printed, displayed, copied, etc. Persons requiring legitimate access to such facilities must be duly authorised and where necessary, cleared to the highest classification of information being processed. The following is a minimum set of personnel security issues that should be considered in each combined system's security policy.

NATIONAL MAPPING

1202. The following table provides details of the national lead authority for any clarification required on this topic.

	AUS	CAN	NZ	UK	US
Lead Authority	DSA DISSP	D IM Secur	DJCIS ISEC	DGS&S InfoSy(Pol)	Joint Staff J65C

MEASURES REQUIRED

1203. All persons who have access to sensitive CIS should have the appropriate clearances and formal access approval for the systems, including a need-to-know. The principle of assigning the least privilege necessary for a user to accomplish his task should be adopted in personnel security procedures.

1204. All Personnel Security activities in an Allied and Coalition context will be handled in line with existing national procedures and CJM3IEM (Combined Joint Multilateral Master Military Information Exchange Memorandum of Understanding). To that end, the following personnel security concerns exist with regard to CIS:

a. **Breaches of Security.** Procedures must be in place for identifying, reporting and managing breaches of security,

b. **Classification by Users.** Originators of information are responsible for the classification of that information,

c. **Clearances and Authorisations.** The System Sponsor(s)/Owner(s) are to ensure that all users of the IT system have appropriate clearance, briefings and authorisation to the highest level of data processed/stored on the CIS or commensurate with the Mode of Secure Operation,

d. **Passwords.** Users are to ensure that passwords are protected outside the system to a level commensurate with the classification of the system,

e. **Separation of Duties.** One of the greatest threats to a CIS is from authorised users. Therefore, the specification and enforcement of user roles and the allocation of responsibilities between these roles (e.g., operator, system administrator or security officer) is a critical security principle which must be considered, to minimize conflict of interest situations. Whenever possible, duties should be assigned in such a way that collusion between two or more people would be necessary before information could be acquired surreptitiously, and

f. **Training and Awareness.** Education is an instrumental tool in the effort to provide adequate IA. Programs must be implemented which instruct personnel as to what security measures are in effect on the CIS they use, why they are required, how they are invoked. Furthermore, all individuals must be trained on how to meet their responsibilities in system security.

CHAPTER 13

PHYSICAL SECURITY

OVERVIEW

1301. All information and CIS hardware shall be physically protected to minimize the likelihood of unauthorised access to the CIS entry points, to sensitive information on the system, as well as to sensitive assets.

NATIONAL MAPPING

1302. The following table provides details of the national lead authority for any clarification required on this topic.

	AUS	CAN	NZ	UK	US
Lead Authority	DSA DISSP	D PM Secur	DJCIS	DGS&S InfoSy(Pol)	Joint Staff J6K

MEASURES REQUIRED

1303. All physical security on which a CIS relies is to be implemented in accordance with participating member nations national policy and standards, as defined by their respective security authorities, and in accordance with any applicable bilateral or multinational agreements. The following sample measures are a minimum set of physical security issues that should be considered when implementing physical security for a CIS or facility:

a. **Perimeters and Security Zones.** These need to be supported by Sentries, Patrols and Intrusion Detection systems. No one shall operate any sensitive equipment in a Public Access or Reception Zone;

b. **Access Controls.** Provision of appropriate identification and authentication. Uncleared or unscreened personnel shall be escorted and provided a visitor's pass; all staff should challenge any unescorted visitors to their facilities;

c. **Secure Containers and Rooms.** Removable hard disk drives and other removable media containing sensitive information shall be secured in approved containers during silent hours; and

d. **Offsite Facilities.** Any remote location used to store backup media or equipment must comply with national policy for the storage of these types of sensitive assets.

CHAPTER 14

ALERTING, WARNING AND RESPONSE

OVERVIEW

1401. Most of the activities identified within this publication relate to a proactive security regime, which can be planned and scheduled in advance. There is also a need for a reactive security regime, to address those issues that occur on a more dynamic basis, which are referred to as the AWR activities:

a. **Alerting.** Detecting that something has happened and notifying necessary authorities *and/or* passing any threat and vulnerability information to necessary authorities;

b. **Warning.** Promulgating threat and vulnerability information; and

c. **Response**. Dealing with an incident.

INTERNATIONAL COMPUTER COORDINATION WORKING GROUP (ICCWG)

1402. AWR activities between the AUS/CAN/NZ/UK/US nations are subject to specific MOUs, and are staffed through the ICCWG. CCEB policy on AWR aspects therefore relies on the work of the ICCWG. Documents produced by the ICCWG are detailed at Annex B.

PRINCIPLE

1403. It is essential that real or suspected incidents are reported immediately to respective national CIRTs and/or Allied CIRT so that responsible authorities can take immediate action, if warranted, to prevent further compromises of information and begin the recovery and restoral process.

NATIONAL MAPPING

1404. The following table provides details of the national lead authority for any clarification required on this topic.

	AUS	**CAN**	**NZ**	**UK**	**US**
Lead Authority	ADFCSIRT	CFIOG DND CIRT	DJCIS ISEC	DGS&S JSyCC	US STRATCOM JTF-CNO

MEASURES REQUIRED

1405. All AWR activities in an Allied and Coalition context will be handled in line with existing national procedures:

a. Reports of detected or suspected incidents or vulnerabilities should be made to the appropriate national contact point for the theatre of operations. Types of Incidents that will need to be handled include, but are not limited to:

(a) Malicious Mobile Code (MMC), including viruses, worms and trojans,

(b) Account break-ins and root compromises,

(c) Electronic Attack (EA) including hacking, and

(d) Loss or theft of classified information or equipment;

b. Warnings of new threats and vulnerabilities will be passed through national chains of command; and

c. Incident Response and Investigation (IRI) will progress in accordance with standard operating procedures as defined by ICCWG.

1406. The respective Alliance CND organisations are to be advised all interconnected systems, including what services are supported, 24/7 POC for implementing operation configuration changes and a source as to where operational/business impacts may be gained in a timely manner.

ANNEX A
RELATED PUBLICATIONS

CCEB PUBLICATIONS

Reference	Title	Date / Status
CJM3IEM	Combined Joint Multilateral Master Military Information Exchange Memorandum of Understanding	TBD

ICCWG PUBLICATIONS

Reference	Title	Date / Status
ICCWG Pub 2002(1)	Memorandum of Understanding (MOU) for Computer Network Defence (CND)	Draft
ICCWG Pub 2002(2)	Terms of Reference for the International Computer Network Defence Working Group (ICCWG)	Draft
ICCWG Pub 2002(3)	International Computer Network Defence Standard Operating Procedures (SOP)	Draft

MSAB PUBLICATIONS

Reference	Title	Date / Status
MSAB Publication 1	Terms of Reference for the Multinational Security Accreditation Board (MSAB),	7 March 2003
CAP	Common Accreditation Process (CAP)4	Draft 5.1 1 May 2000

[4] Formerly DITSWG CAP

ANNEX B
ACCREDITATION REFERENCE SHEET AND EVIDENCE STATEMENT

ACCREDITATION REFERENCE SHEET AND EVIDENCE STATEMENT		
System Name		
System Profile	e.g., LAN	
Security Mode of Operation	e.g., Dedicated	
Sensitivity	e.g., CONFIDENTIAL	
Position	**Name**	**Phone**
Project Manager		
IA Specialist		
ISSO		
CIS Manager		
Telecom Officer		
Operational Command		
Additional positions (*if required*) *(also describe the specific task required)*		
Certification Authority		
Accreditation Authority		

Checklists	**Status (or N/A)**	**Responsible Authority**	**Target Date**
System Documentation			
Threat and Risk Assessment		ISSO	
System Description		ISSO	
Multi-national Security Policy		SWG	
Physical Security Documentation			
Physical Security Checklist		SWG	
Personnel Security Documentation			
Personnel Security Checklist		SWG	
IT Security Documentation			
COMPUSEC Checklist			
Identification & Authentication		SWG	
Detection & Surveillance - Auditing		SWG	
EMSEC Checklist			
CRYPTOSEC Checklist			
TRANSEC Checklist		SWG	
NETSEC Checklist			
Procedural Security Documentation			
Procedural Security Checklist		SWG	
Contingency Planning		SWG	

ANNEX C
MULTINATIONAL SECURITY POLICE TEMPLATE

1. A Multi-national Security Policy (MSP) is composed of three main sections:

a. The general security policy for an organisation, such as the CCEB;

b. An Annex describing the security policy for a specific system, such as the Griffin 5-Eyes network; and

c. Appendices describing the security aspects of each service provided by the system, such as email with attachments.

General Security Policy

2. A general security policy should provide sufficient information to describe the security principles governing the formation and operation of the organisation. It should therefore include the following details:

a. Basic Information describing the organisation and its purpose, including:

(1) Background, and

(2) Scope of Accreditation outlining the accreditation strategy, roles and responsibilities to be followed by the organisation;

b. Detailed description of the organisation including its structure and management processes.

c. A general Threat Statement describing in outline the threats associated with the organisation;

d. Security Risk Assessment describing the security risks associated with the organisation;

e. Security Management Plan describing how security will be managed within the organisation, including incident handling; and

f. Security Requirements describing the general requirements for security that the organisation will implement.

Annexes

3. An annex should be produced detailing the security aspects of each system or network implemented or operated within or on behalf of the organisation.

a. Basic Information describing the system, including:

(1) Background describing the aim of the system,

(2) Scope of Accreditation outlining the accreditation strategy, roles, responsibilities and boundaries of the system,

(3) Role of the Network/System describing its purpose,

(4) Location of Components,

(5) Asset Valuations, these can be either quantitative or qualitative. Usually this is described in terms of the classification and caveats to be handled by the system,

(6) Security Responsibilities, and

(7) Compliance Audit and Re-accreditation Arrangements.

b. Description of the Network/System. This should provide a detailed technical architecture of the system;

c. Threat Statement, in general this should be a detailed assessment of the threats to the system. This can exist in a separate document outside of the MSP for classification or maintainability reasons, but should be referenced within the MSP;

d. Security Risk Assessment describing the security risks associated with the system;

e. Security Management Plan describing how security will be managed during the operation of the system; and

f. Security Requirements describing the general requirements for security that the system will implement.

Appendices

4. An appendix should be produced detailing the security aspects of each service provided or used by the system or network:

a. Basic Information describing the service, including:

(1) Background describing the objectives and reasons for the service operating on the system,

(2) Location of principal Components, and

(3) Compliance Audit and Re-accreditation Arrangements;

b. **Description of the Service.** This should provide a detailed technical architecture of the service;

c. Security Risk Assessment describing the security risks associated with the service and any associated vulnerabilities that may impact other approved services associated with the system; and

d. Security Requirements describing the requirements for security that the service will implement.

GLOSSARY OF TERMS AND ABBREVIATIONS

Access Control

The prevention of unauthorised use of a resource, including the prevention of use of a resource in an unauthorised manner. (NATO)

Accountability

The property that ensures that the actions of an entity may be traced uniquely to the entity. (NATO)

Accreditation

a. The authorisation and approval granted to a data processing system network to process classified information in its operational environment. (NATO)

b. Accreditation is the official management authorisation to operate a CIS or network:

(1) for a specified period of time,

(2) in a particular security mode,

(3) with a prescribed set of administrative, environmental and technical security safeguards,

(4) against a defined threat and with stated vulnerabilities and countermeasures,

(5) in a given operational environment,

(6) under a stated operational concept,

(7) with stated interconnections to other CIS or networks, and

(8) at an acceptable level of risk for which the accrediting authority has formally assumed responsibility. (CA)

Approval to Operate

A temporary approval, granted normally when the certification and accreditation process has been followed, but staffing, certification activities, documentation, or testing is incomplete or outstanding. There may or may not be a higher residual risk to be assumed by the Departmental Security Official. Implicit in the approval to operate is an agreement by the operational authority to action the outstanding items prior to the expiry of the approval to operate. (CA)

Assurance

The confidence that a system or product or a feature of a system or product is free from vulnerability. (NATO)

Audit

The process of conducting an independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, and to recommend any indicated changes in controls, policy, or procedures. (CA)

Authentication

Measures designed to provide protection against fraudulent transmission and imitative communication deception by establishing the validity of a transmission, message, station, or individual. (CA)

Availability

The property of being accessible and usable upon demand by an authorised entity. (NATO)

Boundary Protection Device

Any device placed at the edge of a network designed to perform one or more Barrier Functions (BF) to control the nature of interconnection between domains, including what are colloquially referred to as “Firewalls”, Multi-level Secure (MLS) / Multi Security Level (MSL) devices, as man-in-the-loop-sanction Security Release Control Tools (SRCT) and one-way regulators. (UK)

Certification

Formal technical evaluation of security features and other safeguards of an Automated CIS (AIS). Certification supports the accreditation process and establishes the extent to which a particular AIS design and implementation meet a set of specified security requirements. (ACP 167)

Classified information

Information related to the national interest, the compromise of which would reasonably be expected to cause injury to the national interest.

Coalition

Australia, Canada, New Zealand, United Kingdom, United States, and other nations as applicable, collaborating as peers in a coalition operation.

Combined Information Infrastructure (CII)

The shared or interconnected system of telecommunications networks, computers, databases and electronic systems serving the Combined Joint Task Forces (CJTF) information needs. It comprises components of the member nation's National Information Infrastructure (NII), and includes the people who manage and serve the infrastructure, and the information itself. (AU)

Combined CIS

Combined CIS are those that process, store, distribute or communicate information shared among two or more nations.

Commercial-off-the-Shelf (COTS)

Commercially marketed products that normally are used without modification. COTS software is software that is purchased in ready-to-use condition with supporting user documentation and pre-determined licensing and maintenance agreements. Generally intended for use without modification. (CA)

Compromise

A violation of the security system such that an unauthorised disclosure, modification, or destruction of sensitive or classified information may have occurred or that a denial of service condition has been induced. (NATO)

COMPUSEC

The application of hardware, firmware, and software security features to a computer system in order to protect against, or prevent, the unauthorised disclosure, manipulation, modification or deletion of information, or denial of service. (NATO)

COMSEC

The protection resulting from all measures designed to deny to unauthorised persons information of value that might be derived from the possession and study of telecommunications, or to mislead unauthorised persons in their interpretation of the results of such a study. (ACP 167)

Confidentiality

The property that information is not made available or disclosed to unauthorised individuals, entities, or processes. (NATO)

Containment

Containment is the act of stopping the intrusion and preventing or limiting the damage caused by an intrusion. Damage refers to any violation of security policy and includes any unauthorised disclosure, removal, destruction, modification or interruption of information, CIS or assets. The nature of the containment activity will depend upon the type of threat, the potential access to information and resources, and the sensitivity or criticality of the CIS. (AU)

CRYPTOSEC

The application of security measures, including the application of physical security measures to the cryptographic equipment and associated key material, in order to protect against the exploitation of information during transmission. (NATO)

Data

Representation of facts, concepts, or instructions in a formalised manner suitable for communications, interpretation, or processing by humans by automatic means. Any representations such as characters or analog quantities to which meaning is, or might be, assigned. (AU)

Dedicated Security Mode of Operation

A security mode of operation in which all individuals with access to the data processing system or network are cleared to the highest classification level of information stored, processed, or transmitted within the data processing, and with a common need-to-know for all of the information stored, processed, or transmitted within the data processing system or network. (NATO)

Defensive Information Operations (DIO)

Processes, synergised with wider activities and plans, designed to ensure effective decision-making by protecting friendly information, information processes and CIS from deliberate attack, and from accidental and naturally occurring events. The DIO process integrates and coordinates policies and procedures, operations, personnel and technology to protect information and to defend CIS. DIO are conducted through IA, physical security, operations security, counter deception, counter psychological operations, counter intelligence, electronic protection and special information operations. (AU)

Denial of Service

The prevention of authorised access to resources, or the delaying of time-critical operations. (NATO)

Detect Attack

Ability to detect and identify threats, attacks or other degrading conditions. Detection may initiate both restoration and response processes and must include accurate threat assessments, indications and warnings (I&W) of potential attacks, an ability to disseminate warnings of adverse conditions, and timely current intelligence support in the event of an actual attack. This support will involve the ongoing monitoring of appropriate networks and systems to detect disruptions, intrusions and attacks. (AU)

Detection

Detection is the component that looks for anomalous activity that might indicate intrusions, which are unauthorised personnel or, in the case of CIS, unauthorised programs such as malicious code (e.g., masquerade attempts, viruses, Trojan horses, etc.) attacking the system. Intrusions are a series of activities that attempt to compromise the confidentiality, integrity or availability of a resource. Detection can be performed through a variety of means, including surveillance activities, the use of intrusion detection systems and review of audit logs. (AU)

Disruption

Denial of service or corruption of information resulting from a single event, cause, or source; whether direct or indirect, accidental or intentional, rare or common. (AU)

EMSEC

The component of COMSEC that results from all measures taken to deny unauthorised persons information that may be derived from interception and analysis of compromising emanations from crypto equipment, information processing equipment and telecommunications systems. (ACP 167)

Firewall

A specific type of Boundary Protection Device (BPD), being a software application or a CIS system that acts as a security barrier between two network segments and mediates access between those two networks according to an approved set of rules. (CA)

Gateway

The interconnection between 2 (two) networks with different communications protocols. Gateways operate at the 4th through 7th layers of the Open System Interconnection (OSI) model. (ACP 167)

Incident

In information operations, an assessed event of attempted entry, unauthorised entry, or an information attack on an automated CIS. It includes unauthorised probing and browsing; disruption or denial of service; altered or destroyed input, processing, storage, or output of information; or changes to CIS hardware, firmware, or software characteristics with or without the users' knowledge, instruction, or intent. (DOD)

Information Assurance (IA)

The application of security measures[5] to protect information processed, stored or transmitted in communication, information and electronic systems by ensuring their availability, integrity, authentication, confidentiality and non-repudiation. This includes providing for restoration of CIS by incorporating protection, detection and reaction capabilities. (CCEB)

Information Environment

The aggregate of individuals, organisations or systems that collect, process or disseminate information. It also includes the information itself. (AU)

Information Operations

Actions taken to defend and enhance one's own information and CIS and to affect adversary information and CIS. (AU)

Integrity

The accuracy and completeness of information and assets and the authenticity of transactions. See also data integrity and system integrity:

a. **Data Integrity** - The property that data is being handled as intended and has not been exposed to accidental or intentional modification or destruction; and

b. **System Integrity** – The property that a system performs its intended function in an unimpaired manner, free from deliberate or accidental unauthorised manipulation of the system. (CA)

Multinational Security Accreditation Board (MSAB)

A body authorised jointly by the National Accreditation Authorities to act on behalf of the coalition for endorsing the nationally accredited components of combined CIS and approving connections of national affiliated systems to them.

National Affiliated System (NAS)

System(s) under a nation's control connected to a shared CIS, but not included in it, that process, store or transmit shared information.

[5] Such measures include, as appropriate, those of CompuSec, ComSec, CryptoSec, document security, personnel security, physical security, procedural security, TransSec and EmSec as well as other appropriate security measures. (Taken from Annex to AC/35 (WG/1) WP(95)3 dated 13 Jul 95.)

National Information Infrastructure (NII)

Comprises the nationwide telecommunications networks, computers, databases and electronic systems. The NII includes the Internet, the public switched networks, public and private networks, cable and wireless, and satellite telecommunications. (AU)

Need-to-Know

A criterion used in security procedures that requires the custodians of classified information to establish, prior to disclosure, that the intended recipient must have access to the information to perform his/her official duties). (AUS)

Network Security

The protection of networks and their services from unauthorised modifications, destruction, or disclosure, providing an assurance that the network performs its critical functions correctly and there are no harmful side-effects. (CA)

Non-repudiation

The ability to prove the identity of the sender and receiver of an electronic transmission, as well as to verify the transmission and receipt of the message, so that the parties cannot claim not to have sent or received the transmission. Digital signatures are the current non-repudiation technique of choice for the CCEB.

Operations Security (OPSEC)

A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to:

a. Identify those actions that can be observed by adversary intelligence systems;

b. Determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and

c. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. (DOD)

Personnel Security

The application of security measures, in order to ensure that all personnel who have access to information have the required need-to-know and have the appropriate security clearance. (NATO)

Physical Security

That component of security which results from all physical measures necessary to safeguard equipment, material, and documents from access thereto or observation thereof by unauthorised persons. (ACP 167)

Privacy

The rights of individuals to control or influence what information related to them may be collected and stored, and by whom and to whom that information may be disclosed. (NATO)

Publicly Accessible Network(s)

Network accessible to the general public, such as the Internet. (UK)

Recovery

Recovery is the act of restoring the system to the last known secure state and addressing the vulnerability to prevent the same intrusion from recurring.

Restore Functions

The ability to control the damage that results from an attack and to restore the protected information environment. (AUS)

Risk

a. **Acceptable Level of Risk** - A judicious and carefully considered assessment by the appropriate DAA that an information technology (CIS) activity or network meets the minimum requirements of applicable security directives. The assessment should take into account the value of CIS assets; threats and vulnerabilities; countermeasures and their efficiency in compensating for vulnerabilities; and operational requirements. (Based on OPNAVINST 5239.1A.)

b. **Residual Risk** - The portion of risk that remains after security measures have been applied. (NATO)

Risk Management

The total process of identifying, controlling and minimizing uncertain events that may affect system resources. (NATO)

Secure Managed Interface

One or more BPD forming the control point(s) between combined CIS and NAS. (UK)

Security Architecture

The subset of the CIS or communications system architecture dealing with the security of that system. (NATO)

Security Clearance

An administrative determination by competent national authority that an individual is eligible, from a security standpoint, for access to classified information. (AU)

Sensitive information

Information that requires protection due to the risk of loss or harm that could result from inadvertent or deliberate disclosure, modification, or destruction. The term includes information classified in one of the three security classification categories as well as information about individuals requiring protection under the Privacy Act and information not releasable under the Access to Information Act. (CA)

Sensitivity

The characteristic of a resource that implies its value or importance, and may include its vulnerability. (NATO)

Shared CIS

System(s), including interconnecting networks and supporting infrastructure elements, which process, store and transmit shared information; and over which participating member nations share responsibility for its operation.

System-High Mode of Operation

A security mode of operation in which all individuals with access to the data processing system or network are cleared to the highest classification level of information stored, processed or transmitted within the data procesing system or network, but not all individuals with access to the data processing system or network have a common need-to-know for the information stored, processed, or transmitted within the data processing system or network. (NATO)

Threat

Any potential event or act that could cause one or more of the following to occur: unauthorised disclosure, destruction, removal, modification or interruption of sensitive information, assets or services, or injury to people. A threat may be deliberate or accidental. (CA)

TRANSEC

That component of COMSEC that results from all measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis. (ACP 167)

Trusted Computing Base (TCB)

The totality of protection mechanisms within a computer system, including hardware, firmware and software, the combination of which is responsible for enforcing a security policy. (NATO)

Vulnerability

A weakness or lack of controls that would allow or facilitate a threat actuation against a specific asset or target. (NATO)

Waiver

When a security requirement has been set aside and need not be implemented at all. Security waivers are only to be granted by the NAA if a compelling operational requirement exists. (CA)

ABBREVIATIONS

ACP	Allied Communications Publication
AIS	Automated (Communications and) Information Systems
AUSCANNZUKUS	Australia, Canada, New Zealand, United Kingdom, United States
AWR	Alerting, Warning and Response
BPD	Boundary Protection Device
C-E	Communications - Electronics
C&A	Certification and Accreditation
C4I	Command, Control, Communications, Computers, and Intelligence
CAEC	Coalition Accreditation Endorsement Certificate
CCEB	Combined Communications-Electronics Board
CII	Combined Information Infrastructure
CIS	Communications and Information Systems
CJM3IEM	Combined Joint Multilateral Master Military Information Exchange Memorandum of Understanding
CM	Configuration Management
CND	Computer Network Defence
COMAG	Combined Agreement
COMPUSEC	Computer Security
COMSEC	Communications Security
COTS	Commercial-off-the-shelf
CRYPTOSEC	Cryptographic Security
CTCPEC	Canadian Trusted Computer Product Evaluation Criteria
CWAN	Combined Wide Area Network
DAA	Designated Accrediting Authority
DGS&S	Director General of Security and Safety
DIM SECUR	Director Information Management Security
DIO	Defensive Information Operations
DISSP	Defence Information Systems Security Program
DITSWG	Defence Information Technology Security Working Group (now defunct)
DJCIS	Directorate of Joint Command, Control, Communications Information Systems
DOS	Denial of Service
DSA	Defence Security Authority
DSSO	Defence Security Standards Organisation
EA	Electronic Attack
EDI	Electronic Data Interchange
EMCON	Emission Control
EMSEC	Emissions Security
I&W	Indications and Warnings
IA	Information Assurance
ICCWG	International Computer Network Defence (CND) Coordination Working Group
IM	Information Management
IA	Information Assurance

INFOSEC	Information Security
IO	Information Operations
IRI	Incident Response and Investigation
IS	Information System
ISSO	Information System Security Officer
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria (UK)
KMS	Key Management System
LAN	Local Area Network
LPI	Limited Probability of Intercept
MAN	Metropolitan Area Network
MLS	Multi-level Secure
MMC	Malicious Mobile Code
MOU	Memorandum of Understanding
MSAB	Multi-national Security Accreditation Board
MSL	Multi Security Level
MSP	Multi-national Security Policy
NAA	National Accreditation Authority
NAEC	National Accreditation Endorsement Certificate
NAS	National Affiliated System
NATO	North Atlantic Treaty Organisation
NETSEC	Network Security
NII	National Information Infrastructure
NRPL	NATO Recommended Product List
OPSEC	Operations Security
PAN	Publicly Accessible Network(s), such as Internet
PKI	Public Key Infrastructure
SA	Security Authority
SCIF	Secure Compartmented Information Facility
SDA	Sensitive Discussion Area
SIGINT	Signals Intelligence
SMI	Secure Managed Interface
SOA	System Operating Authorities
SRCT	Security Release Control Tools
SSA	Secure SIGINT Area
SSP	System Security Policy
ST&E	Security Test and Evaluation
SWG	Security Working Group
TCB	Trusted Computing Base
TCSEC	Trusted Computing System Evaluation Criteria (US)
TORs	Terms of Reference
TRA	Threat and Risk Assessment
TRANSEC	Transmissions Security
TSI	Technical Security Inspection
VA	Vulnerability Analysis
WAN	Wide Area Network

WG	Working Group
WS	Washington Staff