

UNCLASSIFIED

COMBINED FEDERATED BATTLE LABORATORIES NETWORK (CFBLNet)



PUBLICATION 1 ANNEX C APPENDICES

CFBLNET SECURITY AND INFORMATION ASSURANCE STRATEGY

**Version 6.0
October 2009**

UNCLASSIFIED

DOCUMENT CONTROL AND TRACKING METADATA

Security Classification	Unclassified
Access Status	Version 6.0
Usage Condition	Publicly Releasable

Scheme Type	CFBLNet Documentation Control and Tracking Scheme
Scheme Name	See Pub 1, Annex G, CFBLNet Document Management
Title Words	CFBLNet Pub 1 – Annex C, Appendices, CFBLNet Security and Information Assurance Strategy

Function Descriptor	Security and Information Assurance Strategy
Activity Descriptor	Informational

Event Date	Agent Type	Agent Name	Agent Details	Event Type	Event Description
30Oct09	C-EG	Steve Pitcher	C-EG Chair	Review/Approve Sign	Publication 1, Annex C, Appendices, Version 6.0

TABLE OF CONTENTS

APPENDIX 1 – CFBLNET RISK ENVIRONMENT AND MITIGATION STRATEGY	5
Security Environments	5
Risk Management	6
Risk Management Responsibilities.....	6
Principles.....	6
Terminology.....	6
Threats to the CFBLNet	7
Introduction.....	7
Threats.....	7
Threat Agent Classes	7
Threat Agent Methods of Attack	8
Threat Mitigation	9
CFBLNet Vulnerabilities and Counter-Measures	10
Introduction.....	10
Vulnerabilities and Counter-Measures.....	10
APPENDIX 2 – CFBLNET SITE INTERCONNECTION APPROVAL GUIDELINES ...	20
Introduction	20
PART 1. BOUNDARY PROTECTION SYSTEMS DESCRIPTION	21
Unique Interconnection Identifier Number:	21
External Interconnections	21
PART 2. EVIDENCE OF INTERCONNECTION COMPLIANCE STATEMENT	22
PART 3. COMPONENT/HOST CONFIGURATION INFORMATION	23
PART 4. INTERCONNECTION APPROVAL CHECKLIST	24
APPENDIX 3 – CFBLNET INITIATIVE CONNECTION APPROVAL GUIDELINES ..	26
Introduction	26
PART 1. SYSTEMS ARCHITECTURAL DESCRIPTION	27
Internal and External Connections.....	27
Local Connection	27
Security of Gateways	27
PART 2. EVIDENCE OF COMPLIANCE STATEMENT	28
PART 3. COMPONENT/HOST CONFIGURATION INFORMATION	29
PART 4. CONNECTION APPROVAL CHECKLIST	32
PART 5. CFBLNET ACCESS ASSESSMENT	34

APPENDIX 4 – MSAB NATIONAL ACCREDITATION ENDORSEMENT PROCESS . 36
**APPENDIX 5 – MSAB NATIONAL ACCREDITATION ENDORSEMENT
CERTIFICATE (NAEC) TEMPLATE 37**
APPENDIX 6 – CLASSIFICATION GUIDANCE FOR THE CFBLNET..... 38
1. Introduction..... 38
2. Guidance..... 38

APPENDIX 1 – CFBLNET RISK ENVIRONMENT AND MITIGATION STRATEGY

Security Environments

101. CFBLNet Community Security Environment (CSE). The CFBLNet is viewed as a community, that is to say a system of systems. While each individual system is logically distinct and physically separate from other CFBLNet systems, the principal function of each CFBLNet element (workstation, server, router, node, gateway, network, etc.) is to support the exchange of information. The CSE is the general security environment that identifies where security measures are to be enforced, which contribute to the protection of the CFBLNet CIS as a whole.

102. The CSE for the CFBLNet CIS cannot be defined in terms of physical boundaries (e.g., a perimeter fence or walls of a building). It is only possible to define the CSE in terms of a logical entity, or concept, that is the ‘sum’ of its contained parts. The overall CSE embraces the Global Security Environment (GSE) of each Coalition element, which further contains the Local Security Environment (LSE) and the Electronic Security Environment (ESE). While the boundary of the CSE can only be described in logical terms, the boundary of a GSE, LSE or ESE follows a physical boundary.

103. CFBLNet Global Security Environment (GSE). The GSE of each system within the community consists of the outermost perimeters of the establishment, which ‘houses’ the system. The security of these establishments shall be under the authority of a designated security officer (e.g., post, camp, station, ship security officer or national/organization team leader).

104. CFBLNet Local Security Environment (LSE). The LSE consists of areas over which the system managers within the community have control, which may in turn be exercised through the security officer of the establishment (GSE) within which the LSE resides. In some cases, the GSE and LSE of some CFBLNet sites will be identical. The LSE of any CFBLNet element shall meet the requirements of a NATO Class I/II facility, or national equivalent area.

105. CFBLNet Electronic Security Environment (ESE). The ESE consists of any element (workstation, server, router, node, gateway, local area network, etc.) within the CFBLNet boundary that stores, processes and/or transmits CFBLNet information.

Risk Management

Risk Management Responsibilities

201. Risk management on the CFBLNet is the shared responsibility of each CMP in order to maintain the confidentiality, integrity and availability of the CFBLNet, in accordance with the CFBLNet Technical Arrangement (Charter).

202. Each CMP is responsible for carrying out the risk assessment of its own infrastructure; the risk assessment methodology used is at the discretion of the CMP performing the task. A risk assessment is subject to update when additional interconnections are being considered or significant changes are being proposed to a given infrastructure.

203. The risk assessment process is a part of the certification and accreditation (C&A) process for both sites and Initiatives, including sponsored non-CFBLNet nations/organizations. The security accreditation authority for each CMP shall identify any risks that impact upon the security of the network.

Principles

204. Risk management is the approach of identifying the level of risk associated with information compromise and mitigating that risk to an acceptable level to achieve optimum operational effectiveness or business function. CFBLNet is committed to a policy of risk management. Risks to the CFBLNet information will be categorically identified, ranked by relative severity, and then countered in priority order, based upon available resources. The decision on whether or not the CIS can be operated in the manner proposed will be based on the residual risk (risk remaining after countermeasures have been put in place). The CFBLNet community acknowledges that some risk of compromise is inherent during the operation of any information system.

Terminology

205. The following risk management terms will be used in this document (individual CMP may use different terminology):

- **Risk** is the probability of occurrence of a threat exploiting a vulnerability, resulting in a negative impact on an asset.
- **Assets** are all the components used within a CIS that contribute to the accomplishment of an organization's goals. Assets are categorized as information, functional, or physical.
- **Vulnerability** is a design, administrative, or implementation weakness or flaw in a CIS asset that, if exploited, could lead to an unacceptable impact.
- **Threat** is a person, event, or circumstance with the potential (motivation, capability and opportunity) to capitalize on a vulnerability, causing harm to a CIS asset, in the form of destruction, disclosure, degradation of data, or denial of service.
- **Safeguards** are processes, procedures, techniques, or features intended to mitigate the negative effects to CIS assets through the exploitation of vulnerabilities by threat agents.
- **Residual Risk** is the risk that remains after you apply safeguards to a CIS.

Threats to the CFBLNet

Introduction

301. A degree of risk is inherent with connecting multiple CMP systems and with multiple CMP systems sharing a common resource (the CFBLNet). This chapter describes the threats associated with these connected and/or shared systems.

Threats

302. In assessing the risks to CFBLNet several classes of threat agents and attack methods must be considered. When calculating the risk to a system associated with any given threat agent or method of attack, it is important to also consider the resulting impact to the system, and the likelihood of that attack occurring.

303. Because the precise threat environment is dynamic, these detailed threat factors will be considered by the appropriate national accreditation authorities, MSAB and the CFBLNet Security Working Group on a per-Initiative basis.

Threat Agent Classes

304. There are three primary characteristics that define a threat agent: where the threat originates; the intent of the agent; and the capabilities of the threat agent. Each of these characteristics can take one of two values thus leading to eight possible threat agent classes. The definitions of these threat classes are as follows:

- a. The **internal, non-hostile, unstructured (INU)** threat is an individual within the CFBLNet CIS who normally has physical access to network components. This individual is not motivated to disrupt CFBLNet operations but can do so unknowingly. This threat does not have any unusual skills or tools, and is not interested in attacking.
- b. The **internal, non-hostile, structured (INS)** threat is an individual within the CFBLNet CIS who normally has physical access to network components. This individual is not motivated to disrupt CFBLNet operations but can do so by making common mistakes. The INS threat is usually quite skilled and has a number of tools that can assist them in performing security related functions. System administrators, network engineers and technical staff associated with demonstrations fall into the INS threat category.
- c. The **internal, hostile, unstructured (IHU)** threat is an individual within the CFBLNet CIS who normally has physical access to network components. This individual is motivated to disrupt the operations of CFBLNet but lacks the resources, tools, or skills necessary to launch a sophisticated attack. It would not be unusual for this type of threat to mount an attack on the CFBLNet by deploying a common virus. Unskilled disgruntled users that could benefit from disrupting operations fall into the IHU threat category.
- d. The **internal, hostile, structured (IHS)** threat is an individual or group within the CFBLNet CIS who are motivated to disrupt CFBLNet operations or exploit

- vulnerabilities to assets. This type of threat has significant resources, tools, and skill to launch a sophisticated attack and potentially remove any evidence of the attack. Due to the open nature of CFBLNet, the IHS threat is least likely to act but has the greatest potential to cause damage. Highly skilled CFBLNet technicians (e.g. system administrators) or technical demonstrators that could benefit from disrupting operations or attempting to obtain commercially sensitive information fall into the IHS threat category.
- e. The **external, non-hostile, unstructured (ENU)** threat is an individual who is not within the CFBLNet CIS and has little or no motivation for mounting an attack. This threat has limited resources, tools, skill, or funding to launch a sophisticated attack. Common Internet users fall into the ENU threat category.
 - f. The **external, non-hostile, structured (ENS)** threat is an individual outside the CFBLNet CIS, who has little or no motivation for attacking the network. However, this threat has special resources, skills, tools, or funding to launch a sophisticated attack. System and network security professionals that use the Internet to obtain information or improve their skills fall into the ENS threat category, as do similar individuals associated with external national systems.
 - g. The **external, hostile, unstructured (EHU)** threat is an individual outside the CFBLNet CIS who is motivated to attack and exploit or disrupt CFBLNet operations. This individual has limited resources, tools, skill, and funding to successfully accomplish a sophisticated attack. Many Internet hackers, most crackers and vandals fall into the EHU threat category.
 - h. The **external, hostile, structured (EHS)** threat is an individual or group outside the CFBLNet CIS who are motivated to attack and exploit or disrupt CFBLNet operations. This threat has substantial resources, unique tools, is highly funded and extremely skilled. Hostile intelligence services, criminal elements, and professional hackers involved in information warfare, criminal activities or industrial intelligence often fall into the EHS threat category.

Threat Agent Methods of Attack

305. There are several ways in which threat agents may act. An attack method has 3 characteristics, one from each of the following pairs:

- a. Accidental or Deliberate;
- b. Active or Passive;
- c. Logical or Physical.

306. An **accidental** compromise occurs when a threat agent inadvertently discloses information to someone that should not know it, or mistakenly modifies some important information in an inappropriate way. For example, a user might sanitize a Secret document with the intention of sending this to someone not cleared for Secret, but then accidentally attaches the original file to the message. This type of compromise is not necessarily performed by a person. For example, a piece of hardware might fail in an 'open' state, rather than in a 'secure' state. This characteristic includes natural disasters, hardware failures and other unexpected, unintended occurrences.

307. A **deliberate** compromise occurs when a threat agent intentionally performs an action that is unauthorised. For example, a user removes an audit file from the system to remove evidence of which applications he has been running.

308. An **active** attack results from the user performing an action. For example, an attacker may compromise information by exploiting a flaw in the implementation or configuration of the system, then use this flaw to allow additional illicit services to pass through the firewall, such as Telnet.

309. A **passive** attack occurs when the user does not perform an action which would otherwise protect the integrity, confidentiality or availability of the system. For example, a system administrator may fail to adequately rotate log files, causing the hard disk to fill and the system to fail.

310. A **logical** attack is an attack which affects the confidentiality, integrity or availability of the CIS through electronic means. For example, an attacker may cause a denial of service by flooding a web server with requests, or an attacker may send a user a document which, when opened, executes some macros that email the user's most sensitive documents back to the attacker.

311. A **physical** attack results from the actual tampering with or destruction of CIS equipment, and requires physical access to the computer facilities. Physical attacks include the flooding of a server room, the dropping of a server or the shredding of required documents, for example.

Threat Mitigation

312. The threat of sabotage or espionage is considered remote due to the limited amount of real world information to be transmitted on the CFBLNet CIS and lack of real world impact. However, all participants should exercise a high degree of vigilance and security awareness when involved in an Initiative. All participants are responsible for exercising strict personnel security discipline. They shall notify the site security officer of any suspicious persons or incidents. Some examples of reportable incidents are:

- a. Attempted surreptitious entry to a facility.
- b. Attempted bypass of system passwords.
- c. Unexplained modifications to equipment.
- d. Unexplained changes to or loss of data in a system.
- e. Missing equipment or software.

313. Comprehensive security awareness programs and thorough training for personnel using, and especially configuring, the CIS are necessary to reduce the risk associated with non-hostile threat agents.

CFBLNet Vulnerabilities and Counter-Measures

Introduction

401. All CIS systems are vulnerable – the degree of vulnerability increases with the complexity of the system. More moving parts makes a system more vulnerable to physical failure, highly sensitive data make a system more vulnerable to unauthorized access attempts.

402. The vulnerabilities of each system in the CIS are promulgated to all nations of the CFBLNet community due to the connectivity of systems. The success of the CFBLNet requires a high degree of trust among the participants that a mutually-acceptable baseline of security exists across the CIS. While this document outlines what is required within the CFBLNet community, national directives for the secure operation of classified networks remain the prime reference documents. If the requirements listed in this document are more restrictive than national directives, it is assumed that this document will take precedence.

403. Each CMP will perform the following:

- a. Conduct Vulnerability Assessment (VA) of their own sites and Initiatives.
- b. When a CMP believes they have identified a vulnerability that affects the CFBLNet assurance, they have an obligation to inform the remaining CMP, unless it is in contradiction to its National Security Policy or proprietary agreements.
- c. There is an obligation on Initiative Sponsors to inform industry participants in CFBLNet Initiatives that vulnerability assessment may be conducted on those Initiatives. Therefore, Intellectual Property Rights (IPR) for new Initiatives are not necessarily protected.

Vulnerabilities and Counter-Measures

404. This section outlines broad areas of vulnerability that have been identified within the CFBLNet CIS and provides suggested methods of reducing the impact or exploitability of these vulnerabilities. The recommended Level of Assurance associated with each of these vulnerability areas is also discussed. The vulnerabilities and counter-measures identified in this section are applicable to all assets that are within the boundary and scope of the CFBLNet.

405. **Identification and Authentication.** All individuals with a “need to know” and systems with access to the CFBLNet CIS shall be reliably identified and their authorization established. All automated processes operating on behalf of an individual shall be unequivocally associated with that individual.

- **Vulnerability**

Individuals may gain access to information for which they do not have clearance or need to know, or perform operations without being held accountable.

- **GSE/LSE Counter-measures**

Site Directors will restrict access to all network equipment and classified CIS processing areas and equipment to persons cleared to at least the National/NATO

SECRET level. Site Directors will implement positive access controls. Unclassified presentations to the Press, non-Coalition visitors, and other visitors with an interest in the CFBLNet but lacking appropriate security clearance or “need to know” may be accommodated by sanitizing the Initiative areas of classified information and maintaining cleared escorts for the visitors.

- **ESE Counter-measures**

Information systems security (INFOSEC) measures ensuring identification and authentication for all users shall be implemented on all systems providing access to the CFBLNet CIS.

All users of the CFBLNet CIS shall be positively and uniquely identified (locally) at the beginning of a process session.

Passwords or stronger mechanisms are to be used for authentication of users for the protection of confidentiality, and system/data integrity and availability. Group passwords are not permitted. Passwords will have a minimum length of 8 characters and should contain both alphabetic and non-alphabetic characters and be case sensitive.

The origin of each e-mail item shall be identified for each mail exchange.

- **Level of Assurance**

No specific level of assurance is required for Identification and Authentication measures, except for those systems, which operate under “trusted” operating systems (i.e., EAL4 and higher or national/NATO equivalent).

406. **Access Control.** Access shall be limited to participants and visitors with appropriate clearances and “need to know”.

- **Vulnerability**

Unauthorized users may intentionally or accidentally gain access to CFBLNet data.

Authorized users may intentionally or accidentally gain unauthorized access to functions and privileges.

Authorized users may intentionally or accidentally import unauthorized software into the CFBLNet CIS.

- **GSE/LSE Counter-measures**

The identity and clearance of visitors must be established before allowing them access to classified information. Personnel without proper security clearances will only be allowed access to classified CFBLNet areas on an exception basis, and only

with the authorization of the National/Organization Initiative Lead and prior sanitization of the area to be visited.

When visitors do not hold an appropriate security clearance for the information used by the Initiative they are visiting, escort officials will ensure that personnel at each demonstration being visited are aware of the upcoming visit and given time to sanitize the area of non-releasable and/or other classified material.

The Site Director will ensure adequate security measures for the operation and storage of classified material is available at an Initiative site.

Participants will keep classified printed material to an absolute minimum. They will destroy classified products generated for the Initiative at the earliest feasible time, when they are no longer required. All participants will comply with national/NATO/service/agency/command regulations for printed and electronic classification marking.

Sites are responsible for providing approved shredders/destruction devices appropriate to the classification level to destroy classified printed output. Participants will use approved destruction devices listed in national/NATO/service/command/agency COMSEC regulations for destruction of COMSEC material.

- **ESE Counter-measures**

It shall not be possible for users to access any of the functions, features and capabilities of any elements of the CFBLNet CIS without being identified.

All users shall have a unique user ID and password.

Access privileges shall be implemented to ensure that applications and system functions are only available to authorized users.

Only three consecutive unsuccessful login attempts to gain access to the CFBLNet CIS are to be allowed. If the third login attempt fails, the following actions are to be taken:

- a. the user identity is to be locked out until reset by the system administrator;
- b. the reason for the failure is not to be displayed at the terminal where the attempt is made;
- c. failure of the user to gain access is not to result in the asset being locked out of the CIS;
- d. means are to be provided so that if all accounts that can force password changes are locked out, authorized persons with physical access to the servers can enable the locked-out accounts; and

- e. on successful login access to a subsystem, the date and time of the user's last successful access is to be displayed.

- **Level of Assurance**

No specific level of assurance is required for Access Control measures, except for those systems that operate under "trusted" operating systems (i.e., EAL4 and higher or National/NATO equivalent).

407. **Accountability.** Users shall be individually accountable for information that is created, modified, deleted or transmitted within the CFBLNet CIS, and thus deter authorized users who are disposed to compromise the data.

- **Vulnerability**

Individuals who are authorized to access the CFBLNet CIS information may misuse that authority to:

- a. perform other security relevant operations (e.g., take unauthorized copies) against the interest of the CFBLNet community, or
- b. breach or attempt to breach the system or network security without being made accountable for their actions.

- **GSE/LSE Counter-measures**

All visitors to CFBLNet sites will be recorded on visitor control rosters.

Physical and other security measures, such as spot checks on exit, are implemented to prevent or deter unauthorized export of hard copy output or electronic storage media.

All computer storage media used to exchange information shall be uniquely identifiable and labeled with the highest security classification contained on the media in accordance with national/NATO/service/agency/command security classification marking regulations.

- **ESE Counter-measures**

All systems within the CFBLNet CIS should maintain an account for security related events that may occur. The security events include:

- a. System start-up and faults.
- b. User log-on (to include log-on attempts) and log-off.
- c. Any access to systems security data.
- d. Diagnostically detected errors.

- e. Unsuccessful attempts to access resources.
- f. Attempted violations of a user's privileges.
- g. Other security related events.

For each security event, the following shall be recorded.

- a. Event type.
- b. Date and time of event.
- c. Success or failure of event.
- d. Identity of the terminal/workstation user.
- e. For events concerning identification and authentication data (e.g., user id or passwords), the origin of the request (e.g., the terminal/workstation identifier).

- **Level of Assurance**

No specific level of assurance is required for Accounting measures, except for those systems that operate under "trusted" operating systems (i.e., EAL4 and higher or National/NATO equivalent).

408. **Audit.** The Audit function monitors security related events to detect and warn of activity that might threaten system and network security, and thus reveal attempted or actual breaches of system and network security.

- **Vulnerability**

Actions, whether by design or accident, which could breach security or lead to a breach of security, may not be detected and measures to prevent or deter further actual or attempted breaches may not be taken.

- **GSE/LSE Counter-measures**

The GSE security organization will inform the LSE security organization whenever an attempted or actual breach of security has occurred – that impacts on their LSE.

The LSE security organization will inform the GSE security organization whenever an attempted or actual breach of security has occurred – that impacts on their GSE.

- **ESE Counter-measures**

Normally, audit reduction tools will be available to assist the ISSO in investigating actual or potential security problems. In the CFBLNet CIS, many of the systems are not sufficiently mature to have had or required such tools be in place, as is normal in operational systems.

Where such tools are in place, they shall be capable of presenting the accounting information in a form that is easily accessed and understood. These tools shall provide support to the following activities:

- a. Accountability of information.
- b. Investigation of actual or potential systems security violations.
- c. Selective examination (retrieval and printing) of accounting files by:
 - i One or more users IDs.
 - ii By event type.
 - iii By date and time ranges.
 - iv Comparison of accounting records.
- d. Selection of audit material using flexible criteria, for long-term retention.

- **Level of Assurance**

No specific level of assurance is required for tools to examine accounts.

409. **Information Marking and Handling.** All information that resides in the CFBLNet CIS shall be associated with an Information Label.

- **Vulnerability**

Operational users may be unaware of the originator of the data and may thus compromise the confidentiality of the data.

Operational users may be unaware of the true classification of the data and may thus compromise the confidentiality of the data.

In the context of the CFBLNet CIS, where all users are cleared to the highest level of the information stored, processed and transmitted, the risk of compromise of CFBLNet information is deemed to be acceptable with implementation of the below GSE/LSE/ESE measures.

- **GSE/LSE Counter-measures**

All information objects (products), as a mandatory requirement, should have an *Information Label*. Any unlabelled information must be treated at the highest classification level with the most restrictive releaseability caveat.

If there is a requirement to identify information at different classification levels within a word processing (WP) document or message then an *Information Label* shall be provided for each paragraph/ section/ Annex/ appendix, as applicable, where the

Protective Marking component shall identify the highest classification of the data contained.

Procedurally, it is the responsibility of the originator to ensure that the *Information Label* is present and gives the correct originator, classification and release.

A change to the *Information Label* shall only be made with the agreement of the originator.

For legacy data prior to endorsement of Annex C, unlabelled data will be handled as (Originator) SECRET Releasable to AUSCANZUKUS and NATO.

Initiative data on the CFBLNet CIS will be retained until receipt of the final report by the CFBLNet Secretariat or 3 months after the end of the Initiative, after which time it will be purged from the network by the respective site manager.

- **ESE Counter-measures**

All documents shall contain the *Information Label* in their 'header' and 'footer'. If there is a requirement to identify information at different classification levels within a word processing (WP) document or message, then an *Information Label* shall be provided for each paragraph/section/Annex/appendix, as applicable, where the *Protective Marking* component shall identify the highest classification of the data contained.

All messages shall follow the agreed formatting rules for the message classification.

All drawings, graphics and overlays shall contain the *Information Label* as 'text lines' that are part of the 'object'.

All spreadsheets shall contain the *Information Label* as 'text lines' that 'top & tail' the spreadsheet.

All binary objects (e.g., imagery) shall contain the *Information Label* as a part of the object itself, when entered into the CFBLNet environment.

- **Level of Assurance**

No specific level of assurance is required for this procedural mechanism.

410. **Data Communications.** It should not be possible to intercept or redirect data communications links in order to compromise the confidentiality or integrity of the CFBLNet CIS.

- **Vulnerability**

Data is misrouted to an unauthorized and/or unidentified system or user by the CFBLNet CIS.

Information transmitted over the CFBLNet CIS may be compromised in terms of confidentiality, authenticity or integrity by passive or active means.

Unauthorized remote access into the CFBLNet CIS that may result in either insertion of unauthorized or malicious software or compromise data in terms of confidentiality, availability or integrity.

Unauthorized systems/personnel masquerade as authorized CFBLNet CIS systems/personnel and thereby compromise the data in terms of confidentiality, availability or integrity.

Unauthorized personnel gain access to routing table data/software and thereby compromise the CFBLNet CIS by Denial of Service (DoS).

The availability and integrity of the data may be compromised by a failure of the CFBLNet CIS.

- **GSE/LSE Counter-measures**

The CFBLNet ‘backbone’ is a private network composed of dedicated lines/communications paths (e.g., ATM or TCP/IP) between switches.

All switches should be only connected to CFBLNet circuits.

All communication switches (e.g., routers, terminal adapters, modems) and cryptographic equipment should be held in secured areas with limited access.

The installation of all CFBLNet electronic equipment and cabling which handle classified information shall meet CMP TEMPEST standards, either through the use of TEMPEST equipment or by housing the equipment in a facility built to TEMPEST (or better) Emissions Security standards.

All data passing over the CFBLNet ‘backbone’, between switches, shall be encrypted in accordance with CMP approved encryption standards.

All data passing over a dial-up connection within the CFBLNet CIS shall be encrypted using CMP approved encryption standards.

Routing information for the CFBLNet ‘backbone’ shall be treated as sensitive unclassified information. When stored on removable media (e.g., diskette), the media shall be labeled as “Unclassified – Sensitive configuration management information” and shall only be available to authorized System Administration staff.

- **ESE Counter-measures**

Access to the host and network switch routing table information shall be restricted to authorized users.

Only the CFBLNet Communications Control Center (CCCC)/Network System Manager or authorized representatives shall be allowed to execute routing table maintenance software.

Communications protocols shall provide recovery mechanisms to preserve the integrity of the data transmitted.

Any detected or suspected COMSEC incident or violation is to be reported to the relevant COMSEC custodian of the material involved. Other CFBLNet participants shall be notified of this type of incident, according to CMP policies.

- **Level of Assurance**

No specific level of assurance is required.

411. **Integrity and Availability.** The Integrity and Availability of the CFBLNet CIS shall be maintained.

- **Vulnerability**

Computer viruses or other malicious code may attack the integrity and availability of CFBLNet data, and thus compromise or undermine CFBLNet operations and security.

Computer viruses or other malicious code may attack the integrity and availability of the CFBLNet CIS, and thus compromise or undermine CFBLNet operations and security.

Users (authorized or not) may accidentally or intentionally invoke activities that result in the denial of system resources or data (loss of availability).

- **GSE/LSE Counter-measures**

All participants should conduct a virus scan of their media before bringing media into the LSE.

All participants shall keep the exchange of media (e.g., diskettes, CDs, DVDs, jump drives etc) to a minimum, consistent with operational demands of the Initiatives.

All incidents of malicious code detection or unintended/unauthorized system activity shall be reported to the local ISSO.

Personnel who are authorized to work on configuration management must be adequately trained on the system, to prevent inadvertently causing a denial of service through mis-configuration of the system.

- **ESE Counter-measures**

Each system capable of running virus protection software will have such safeguards implemented. A virus check should be performed daily, normally at system start up

or prior to the beginning of the execution period. Virus databases will be updated throughout the Initiative, as they become available from the vendor.

- **Level of Assurance**

No specific level of assurance is required for Integrity and Availability measures.

412. **Barriers.** A barrier is a mechanism to be used to protect and prevent CFBLNet information from potential compromise. The possible types of barrier are as follows:

- a. Preventative;
- b. Reactive;
- c. Permissive;
- d. Non-technical.

A **preventative barrier** is one that prevents a compromise from occurring. Such defences are typically required where information is particularly sensitive and the damage that would be caused by a compromise is difficult, or even impossible, to remedy. However, for many barriers within the CFBLNet, this will be too constraining and unnecessarily strong.

A **reactive barrier** is one that allows a compromise to occur, but immediately reacts to it and removes its source. This leaves a small “window of opportunity” for a compromise to be exploited, but often the risk this presents is worth taking given the additional flexibility or ease of implementation found in this kind of defence.

A **permissive barrier** permits a compromise to occur and makes no attempt to detect it, but takes actions which allow recovery should it be discovered by some external means. This kind of defence is only appropriate where risks are low.

The final case is in effect the absence of a technical barrier and is where only non-technical defences, such as physical, personnel and procedural controls, are in place.

413. **Media Control (Storage and Sanitization):**

The minimum standards for Storage Media Control are:

- a. The removal of information stored on magnetic/memory media so the information cannot be harvested at a later date by unauthorized personnel (e.g. hard drive ‘wiping’). This activity shall be performed in accordance with CMP policy.
- b. The storage media can be retained in accordance with National/Organisational policy at the existing protective marking/security classification.
- c. The media can to be destroyed in accordance with National/Organisation Policies.

APPENDIX 2 – CFBLNET SITE INTERCONNECTION APPROVAL GUIDELINES

Introduction

101. This CFBLNet Site Interconnection Approval Guidelines provides guidance on types of information that may be required by the CMPs Accreditation Authority to achieve ATO status. This template, when filled in, should have an appropriate classification marking.

102. The document consists of four parts as follows:

PART 1. BOUNDARY PROTECTION SYSTEMS DESCRIPTION

PART 2. EVIDENCE OF EAL COMPLIANCE STATEMENT

PART 3. COMPONENT/HOST CONFIGURATION INFORMATION

PART 4. INTERCONNECTION APPROVAL CHECKLIST

PART 1. BOUNDARY PROTECTION SYSTEMS DESCRIPTION

103. (This portion of the interconnection approval process describes the total interconnection system, in particular the points that will interconnect into the CFBLNet enclave). When completed each page header and footer shall be appropriately classified.

Unique Interconnection Identifier Number:**External Interconnections**

- a. Uniquely describe the interconnectivity of the system.
- b. Focus on the points of demarcation.
- c. List the type(s) of security devices on the boundary protection system, including topology and diagrams.

PART 2. EVIDENCE OF INTERCONNECTION COMPLIANCE STATEMENT

MEMORANDUM FOR: The Record

Subject: Evidence of Interconnection Compliance Statement

1. This letter of compliance affirms that our National or NATO Agency boundary protection system meets all the requirements outlined in the Combined Federated Battle Laboratories Network (CFBLNet) Security and Accreditation Strategy document and recommendations from the SWG to interconnect our proposed boundary protection system to a CFBLNet enclave. Our boundary protection system is equipped with security devices to safeguard information contained in the enclave.
2. We affirm that our boundary protection system has been properly accredited in accordance with our nations/organisations policy requirements and CFBLNet requirements. Authorized users are aware of the security requirements for safeguarding information on the CFBLNet. Users who are caught performing unauthorized acts will be dealt with under the nations/organisations computer security laws.
3. Point of contact for this action is [indicating a name and phone number].

//Signature//
Authorized Official

PART 3. COMPONENT/HOST CONFIGURATION INFORMATION

104. Table B-1 illustrates a table for collecting vital information on each boundary protection system. This information will be used Nationally/Organisationally and by the CFBLNet SWG to create an accurate picture of the boundary protection system that is sufficient to develop a risk model, determine potential vulnerabilities, and recommend necessary safeguards but need not be disseminated outside the CFBLNet accreditation infrastructure. It is vital that this information be provided, as the decisions on whether to grant approval for interconnection.

Table B-1 Generic System Configuration Information Table

DEVICE/HOST INFO	
Device/Host Name:	
Device/Host IP Address (High): *	
Device/Host IP Address (Low): *	
Device/Host Location:	
Device Make/Model:	
EAL level: *	
SOFTWARE INFO	
Operating System with Version #:	
Server Software: (when applicable)	
Applications/Services Software:	
Protocols:	
Ports:	

* When applicable

PART 4. INTERCONNECTION APPROVAL CHECKLIST**Table B-2 Interconnection Approval Checklist**

INTERCONNECTION APPROVAL CHECKLIST			
Site		Name	
Initiative		Signature	
Building		Date	
ITEMS	REQUIREMENTS	YES	NO
Has your network been approved in accordance with your nation's policy?	Accredited by SAA and endorsed by MSAB.		
Have you completed a system connectivity /Configuration/ Topology/ diagram?	Must include backside connections, IP addresses. Encryption devices. All topology information must be reflected in written documentation.		
Have you conducted security Implementation verification?	Each nation is responsible for conducting both announced and unannounced vulnerability assessments.		
Have you conducted a risk assessment?	The risk assessment must be evaluated and approved by the national/Organisation team leader.		
Have you completed the Interconnection Boundary protection system connectivity /Configuration/ Topology/ diagram?	Must include all connections, IP addresses interconnection devices. All topology information must be reflected in written documentation.		
Have you conducted a risk assessment on your interconnection Boundary Protection Systems	The risk assessment must be evaluated and approved by the national/Organisation SAA and a summary must be provided to the CFBLNet SWG.		

Do you have countermeasures in place to protect your network from unauthorized individuals?	Must have security management devices in place i.e. anti-virus software, audit logs review, password authentication		
User security awareness training	Organisations are responsible for training all personnel with authority to access the CFBLNet		
Warning Banner	Does your Organisation have a warning banner on the portion of your network that will be connected to the CFBLNet?		
Incident Reporting	Do you have established incident reporting procedures in place?		

APPENDIX 3 – CFBLNET INITIATIVE CONNECTION APPROVAL GUIDELINES

Introduction

101. This CFBLNet Initiative Connection Approval Guidelines document provides guidance on types of information that may be required by the CMP Accreditation Authority to achieve ATO status. This template, when filled in, should have an appropriate classification marking. The document consists of five parts as follows:

PART 1. SYSTEMS ARCHITECTURAL DESCRIPTION

PART 2. EVIDENCE OF COMPLIANCE STATEMENT

PART 3. COMPONENT/HOST CONFIGURATION INFORMATION

PART 4. CONNECTION APPROVAL CHECKLIST

PART 5. CFBLNET ACCESS ASSESSMENT

PART 1. SYSTEMS ARCHITECTURAL DESCRIPTION

102. (This portion of the connection approval process describes the total network, in particular the points that will connect into the CFBLNet CIS.) . When completed each page header and footer is to be appropriately classified.

Internal and External Connections

Describe the connectivity of the system

Focus on the points of demarcation

Direct connections from the external system to the CFBLNet

Indicate if BPS are used (including type and locations)

Local Connection

103. The local connections describe the network in detail - description must match the topology of the system.

Security of Gateways

104. The security of gateways discusses plans to secure the gateways. Accreditation boundary (list those networks connected into your network, define the exact boundary of the local operating environment e.g. network is connected to the CFBLNet.

PART 2. EVIDENCE OF COMPLIANCE STATEMENT

MEMORANDUM FOR: The Record

Subject: Evidence of Compliance Statement

1. This letter of compliance affirms that our National or NATO Agency systems meet all the requirements outlined in the Combined Federated Battle Laboratories Network (CFBLNet) Security Strategy document to connect our affiliated systems to the coalition network. Our systems are equipped with security devices to safeguard information on the affiliated systems.
2. We affirm that our systems have been properly accredited in accordance with our nation's policy requirements. Authorized users are aware of the security requirements for safeguarding information on the CFBLNet. Users who are caught performing unauthorized acts will be dealt with under the nation's computer security laws.
3. Point of contact for this action is [indicating a name and phone number].

//Signature//
Authorized Official

PART 3. COMPONENT/HOST CONFIGURATION INFORMATION

105. Table B-3 illustrates a table for collecting vital information on each network host. This information will be used nationally to create an accurate picture of the network architecture that is sufficient to develop a risk model, determine potential vulnerabilities, and recommend necessary safeguards but need not be disseminated outside the national accreditation infrastructure. It is vital that this information be provided, as the decisions on whether to grant approval for connection to the backbone network will depend on its accuracy.

Table B-3 Generic Component/Host Configuration Information Table

DEVICE/HOST INFO	
Device/Host Name: *	
Device/Host IP Address: *	
Device/Host Location:	
Device Make/Model:	
SOFTWARE INFO	
Operating System with Version #:	
Server Software: (when applicable)	
Applications/Services Software:	

* Indicates data, which is optional at this time, but will be necessary at execution. If your site already has this data, please include. All other data is mandatory.

106. Along with the tables described herein, a Host Name to IP Address map or table must be provided to the appropriate national security representative NO LATER THAN 10 days prior to commencement of the scheduled event.

Table B-4 Example 1
Multiple Router Component/Host Configuration Information Table

DEVICE/HOST INFO	
Device/Host Name:	Gw1.lortonlab.navy.us Gw2.lortonlab.navy.us
Device/Host IP Address:	123.33.49.32 123.33.49.64
Device/Host Location: (2)	TB 7, U.S. Naval Laboratory, Lorton, OH
Device Make/Model:	CISCO 7507 Router
SOFTWARE INFO	
Operating System with Version #:	Cisco IOS v12.0
Server Software: (when applicable)	N/A
Applications/Services Software:	Internet Control Message Protocol (ICMP), SNMPv1, Remote login (rlogin), Telnet (UNIX), UDP service

Table B-5 Example 2
Sun Workstation Component/Host Configuration Information Table

DEVICE/HOST INFO	
Device/Host Name:	futureplans.burke.af.us
Device/Host IP Address:	123.33.72.40
Device/Host Location:	Suite 304, USAF Laboratory, Burke, AZ
Device Make/Model:	Sun SPARCstation 20
SOFTWARE INFO	
Operating System with Version #:	SunOS 5.5.1 aka Solaris 2.5.1 (SPARC)
Server Software: (when applicable)	N/A
Applications/Services Software:	Netscape Communicator 4.05 for UNIX, E Mail Protocols (SMTP, X.400), FTP (UNIX), Internet Control Message Protocol (ICMP), Portmapper, Remote copy (rcp), Remote login (rlogin), Remote shell(rsh), RPCBIND, Telnet (UNIX),UDP service.

Table B-6 Example 3
Web Server Component/Host Configuration Information

DEVICE/HOST INFO	
Device/Host Name:	Websrvr.fairfax.army.us
Device/Host IP Address:	1123.33.12.28
Device/Host Location:	Rm 12, Battle Lab, Ft Fairfax, MO
Device Make/Model:	Sun SPARCstation 20
SOFTWARE INFO	
Operating System with Version #:	SunOS 5.5.1 aka Solaris 2.5.1 (SPARC)
Server Software: (when applicable)	Apache Web Server 1.3.1
Applications/Services Software:	FTP (UNIX), Internet Control Message Protocol (ICMP), Portmapper, Remote execution (rexec), RPCBIND, UDP service

Table B-7 Example 4
Multiple MS NT Workstation Component/Host Configuration Information

DEVICE/HOST INFO	
Device/Host Name:	Ops1.fairfax.army.us Ops2.fairfax.army.us Ops3.fairfax.army.us Ops4.fairfax.army.us
Device/Host IP Address:	123.33.12.33 to .36
Device/Host Location: (4)	Rm 12, Battle Lab, Ft Fairfax, MO
Device Make/Model:	PC (IBM-compatible)
SOFTWARE INFO	
Operating System with Version #:	MS WinNT 4.0 workstation SP4
Server Software: (when applicable)	N/A
Applications/Services Software:	MS Office Pro 97, Netscape Communicator 4.05 for Windows, Internet Control Message Protocol (ICMP), login program (generic), MS Windows Sockets (Winsock), NT registry, SNMPv1, UDP service.

PART 4. CONNECTION APPROVAL CHECKLIST

Table B-8 Combined Approval Checklist

COMBINED CONNECTION APPROVAL CHECKLIST			
Initiative Number			
Site		Name	
Project		Signature	
Building		Date	
ITEMS	REQUIREMENTS	YES	NO
Has your enclave/site been approved in accordance with your nation's policy?	Accredited by NAA and endorsed by MSAB.		
Has you completed a system connectivity /Configuration/ Topology/ diagram?	Must include tail end circuit connections, IP addresses. Encryption devices. All topology information must be reflected in written documentation.		
Have you conducted security Implementation verification?	Each nation is responsible for conducting both announced and unannounced vulnerability assessment.		
Have you conducted a risk assessment?	The risk assessment must be evaluated and approved by the national/organization team leader.		
Do you have countermeasures in place to protect your network from unauthorized individuals?	Must have security management devices in place i.e. anti-virus software, audit logs review, password authentication		
Purging/ destruction information	Do you have established procedures in place for purging information from the CFBLNet at the end of the event?		

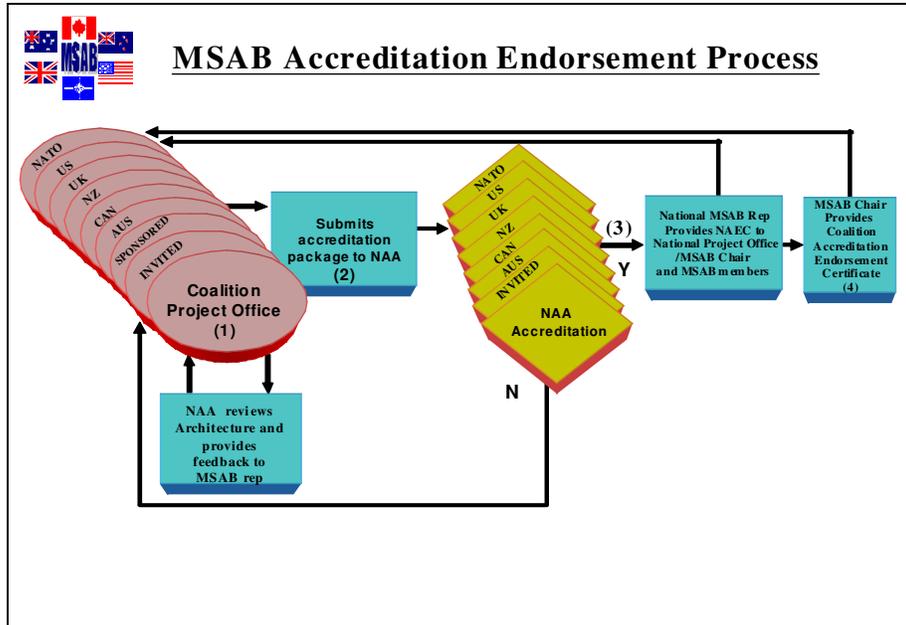
User security awareness training	Organizations are responsible for training all personnel with authority to access the CFBLNet		
Warning Banner	Does your organization have a warning banner on the portion of your network that will be connected to the CFBLNet?		
Incident Reporting	Do you have established incident reporting procedures in place?		

PART 5. CFBLNET ACCESS ASSESSMENT**Table B-9 Who has Access in Specific Areas**

FOREIGN NATIONAL ACCESS			
#1	YES	NO	Foreign Nationals (i.e. non CFBLNet nation personnel), to include Exchange Officers (i.e. non CFBLNet nation personnel in national positions) have physical access to areas where workstations connect directly or indirectly to the CFBLNet. <i>(Example: If other than CFBLNet personnel have access (escorted or unescorted) to the CFBLNet workstation areas, a YES response is required.)</i>
#2	YES	NO	Foreign Nationals (i.e. non CFBLNet nation personnel), to include Exchange Officers (i.e. non CFBLNet nation personnel in national positions) are users on workstations on a network or subnet connected directly or indirectly to the CFBLNet. <i>(Example: If other than CFBLNet. personnel have user accounts on CFBLNet workstations, a YES response is required.)</i>
#3	YES	NO	Foreign Nationals (i.e. non CFBLNet nation personnel), to include Exchange Officers, (i.e. non CFBLNet nation personnel in national positions), are users on workstations on a separate network connected directly or indirectly to the CFBLNet. <i>(Example: A Non-CFBLNet network connected to a CFBLNet connection or using CFBLNet backbone as a transport layer to another Non-CFBLNet. network, a YES response is required.)</i>
CONTRACTOR ACCESS			
#4	YES	NO	Un-cleared contractors have physical access to areas where workstations on the organization network or its subnets connected directly or indirectly to the CFBLNet <i>(Example: Un-cleared contractor personnel, either in support of a Government contract or maintenance support, to include cleaning people, have access to CFBLNet workstations, a YES response is required.)</i>
#5	YES	NO	Un-cleared contractors are users on workstations connected directly or indirectly to the CFBLNet. <i>(Example: Any contractor (Prime or Sub), CFBLNet nation or Non-CFBLNet nation having a user account on the CFBLNet a YES response is required. Explain if the contractor is located within the CFBLNet Government, Non-CFBLNet, Government, or Contractor facility.)</i>
#6	YES	NO	Cleared contractors at a non-military controlled facility are users on workstations connected directly or indirectly to the CFBLNet. Contract Number(s) <i>(Example: Any contractor (Prime or Sub) at a non-national Defence facility (including Contractor facilities) on a separate network such as an Educational Facility, a YES response is required.)</i>
#7	YES	NO	Reference question #6. Are there any un-cleared personnel

			<p>providing support under this contract? <i>(Example: Any contractor personnel (Prime or Sub) that are providing administrative, logistical, or services in support of the contract identified in number 6, a YES response is required.)</i></p>
NETWORK CONNECTIVITY			
#8	YES	NO	<p>The organizational Network, to include subnet(s) and workstation(s), connects to a network operating at any level other than AUSCANZUKUS and NATO SECRET either with or without a high assurance guard in place.</p>

APPENDIX 4 – MSAB NATIONAL ACCREDITATION ENDORSEMENT PROCESS



101. All projects, systems or networks requesting endorsement of the MSAB (inclusive of sponsored and invited nation activities) are required to brief the MSAB during the development process.

- The CMP Project Office submits accreditation package to their CMP Accreditation Authority for approval.
- Sponsored nations are to be accredited by the sponsoring CMP. The appropriate MSAB national representative is responsible for providing the NAEC of any sponsored nation.

102. Invited nations are to be accredited by their National Accreditation Authority to the accreditation policy of one of the MSAB member nations.

- CMP Accreditation Authority is to inform the national MSAB and invited national representative when the system or network is accredited.

APPENDIX 5 – MSAB NATIONAL ACCREDITATION ENDORSEMENT CERTIFICATE (NAEC) TEMPLATE

Multinational
Security
Accreditation
Board



MSAB National ACCREDITATION ENDORSEMENT CERTIFICATE (NAEC)

[From: MSAB National Representative]
[Address]

[Contact Telephone]

[To: MSAB Chair]
[Address]

[Contact Telephone]

(Only For CFBLNet Lead CLR and Secretariat (PMO))

[MSAB Members]

[Nation – Name of Site, System/Network or Initiative]

References:

- A. [National Policy]
- B. Multi-national Security Policy (e.g. CFBLNet Pub 1)

2. This letter certifies that the following *site, system, network or Initiative* has approval to test or approval to operate in accordance with national accreditation procedures (Reference A):

Nation	Site System Network Initiative	Location	Date Issued	Accreditation Expiry Date

2. Highest data classification to be exchanged:

3. The following caveats/restrictions or additional information are noted:

[Caveat/Restriction/MOU]

2. This MSAB NAEC supersedes the previously issued certificate dated xx xx 200x.

[Signed]

MSAB National Representative

[Date]

APPENDIX 6 – CLASSIFICATION GUIDANCE FOR THE CFBLNet

1. Introduction

101. The rationale for classifying aspects of the CFBLNet is based on the potential damage to national security should such information fall into the wrong hands. The CFBLNet and the Initiatives that are conducted on it will have security significance and some aspects will need to be protected accordingly. The following guidance is provided so that the aspects of CFBLNet and any sensitive parts of Initiatives are protected appropriately.

2. Guidance

201. Existence of CFBLNet: **UNCLASSIFIED**

202. Purpose of CFBLNet: **UNCLASSIFIED**

203. Membership of CFBLNet: **UNCLASSIFIED**

204. Specific vulnerabilities and determinations of the CVAT/NVAT activities: **SECRET Rel AUSCANNZUKUS and NATO**

205. Level 0 Topology : **UNCLASSIFIED**

206. Systems and Technical Architecture of the CFBLNet: According to the classification of the respective enclave.

207. IP addresses and specific architecture should be classified in accordance with N/O policy (but can not be lower than Unclassified Not Releasable to the Internet).

208. Key Management: According to the classification of the affected enclave

209. CFBLNet Documentation: **UNCLASSIFIED**

210. Initiative Information: When an Initiative covers a sensitive capability, which requires a higher classification than UNCLASSIFIED, an UNCLASSIFIED synopsis must be produced. The Initiative sponsor will determine the appropriate classification of the Initiative.

211. Funding Issues: National/organizational classification as appropriate.

212. Routing information for the CFBLNet ‘backbone’ shall be treated as unclassified information as long as the complete IP addresses are not shown.

213. Commercially Sensitive Material: To be classified in accordance with the respective national/organizational rules and in accordance with the requirements of the commercial interests involved.