COMBINED FEDERATED BATTLE LABORATORIES NETWORK (CFBLNet)

PUBLICATION 1
ANNEX C
APPENDICES

CFBLNET SECURITY AND INFORMATION ASSURANCE STRATEGY

Version 8.0
July 2015

DOCUMENT CONTROL AND TRACKING METADATA

Security Classification	Unclassified
Access Status	Version .8.0
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
05Sep12	C-EG	Steve Pitcher	C-EG Chair	Review/Approve Sign	Publication 1, Annex C, Appendices, Version 7.0
24Jul15	C-EG	LTC Jacqueline Guillory	C-EG Chair	Review/Approve Sign	Publication 1 Annex C, Appendices, Version 8.0

TABLE OF CONTENTS

APPENDIX 1 – MSAB NATIONAL ACCREDITATION ENDORSEMENT PROCESS

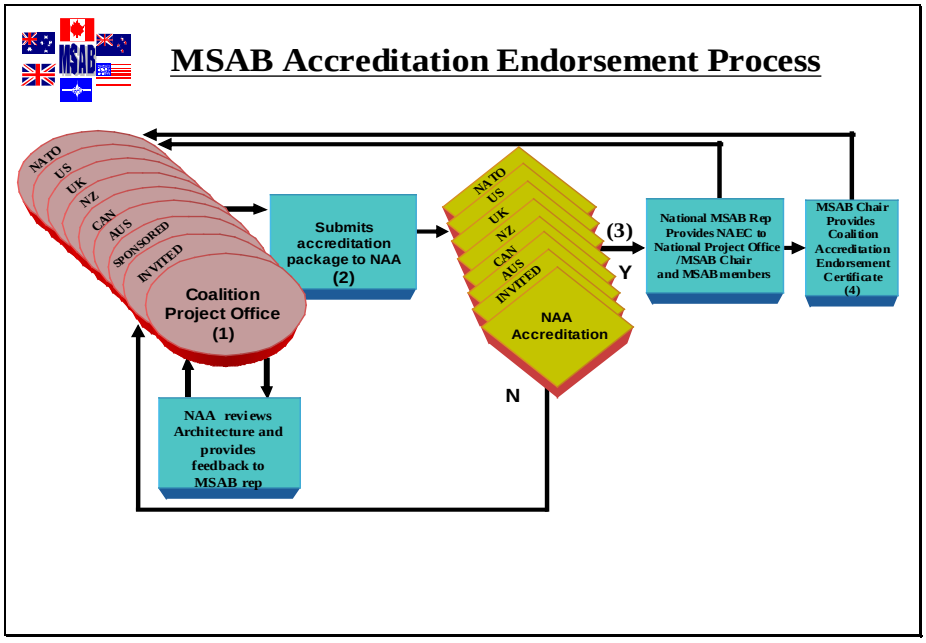

Figure 1 - MSAB Accreditation Endorsement Flow Chart

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.

a. The CMP/GMP Project Office submits accreditation package to their CMP/GMP Accreditation Authority for approval.

b. 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.

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

APPENDIX 2 – MSAB NATIONAL ACCREDITATION ENDORSEMENT CERTIFICATE (NAEC) TEMPLATE

Multinational
Security
Accreditation
Board

MSAB National ACCREDITATION ENDORSEMENT CERTIFICATE (NAEC)

[From: MSAB National Representative] *[Contact Telephone]*
[Address]

[To: MSAB Chair] *[Contact Telephone]*
[Address]

(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)*

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

1. Highest data classification to be exchanged:

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

[Caveat/Restriction/MOU]

This MSAB NAEC supersedes the previously issued certificate dated xx xx 20xx.

[*Signed]*

MSAB National Representative
[Date]

APPENDIX 3 – 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 [and additional Initiative partners when applicable]**

205. Level 0 Topology: **UNCLASSIFIED**

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

206. 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).

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

208. CFBLNet Documentation: **UNCLASSIFIED**

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

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

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

212. 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.

APPENDIX 4 – SECURITY INCIDENT REPORTING

1. Introduction

101. A Security Incident is defined as any event compromising or that has the potential to compromise, the confidentiality, integrity or availability of a communication and information system.

2. Guidance

202. The objective of the reporting process is to provide a framework under which CMP/GMP are able to quickly inform each other of a CFBLNet security incident (including in the context of an initiative). The intent is to:

- Inform partners/participants of initiatives in a timely manner the occurrence of an incident within an initiative.
- Allow first responder/triage of incidents to inform Nations Incident Response/Handling procedures to be invoked.
- Facilitate the inclusion of security incidents in initiative closure reports.

Incident impact category	**Description**	**Action officer (by order of priority)**
Category 1 (possible examples: prolonged network/service outage, extremely widespread malware infection)	The incident may cause severe impact on any users (including users from a different CMP/GMP) of the initiative. The incident may also be related to the possible compromise of classified information	1) CLR 2) Initiative Lead 3) Security WG rep
Category 2 (possible examples: short term network/service outage – cause and remediation are known, local malware infection)	The incident may cause moderate impact on any users (including users from a different CMP/GMP) of the initiative	1) Initiative Lead 2) Security WG rep
Category 3 (possible examples: detected network latency, unexpected IP range)	The incident impact may cause minor impact on any users (including users from a different CMP/GMP) of the initiative	1) Security WG rep

Table 1 - Incident Categories