COMBINED FEDERATED BATTLE LABORATORIES NETWORK (CFBLNet)

PUBLICATION 1
ANNEX C

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, CFBLNet Security and Information Assurance Strategy

Function Descriptor	Security and Information Assurance Strategy
Activity Descriptor	Implementation and Guidance

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, Version 6.0
05Sep12	C-EG	Steve Pitcher	C-EG Chair	Review/Approve Sign	Publication 1, Version 7.0
24Jul15	C-EG	LTC Jacqueline Guillory	C-EG Chair	Review/Approve Sign	Publication 1, Version 8.0

TABLE OF CONTENTS

APPENDICES

Note: All Annex C Appendices are contained in a separate document

CHAPTER 1 – INTRODUCTION

Purpose

101. Annex C to the CFBLNet Pub 1 contains the security management policies, processes and procedures, related to the execution of Initiatives on the CFBLNet, which functions under the authority of the CFBLNet Technical Arrangement / Charter.

102. Annex C provides CFBLNet users with the process for certification and accreditation of CFBLNet sites and Initiatives. This will be done in accordance with the charter member nations/organization Information Systems accreditation policies, directives and processes.

103. Any Initiative using directly or indirectly the CFBLNet infrastructure shall comply with all the security regulations as laid down in Annex C.

Authority

104. Annex C is issued by the CFBLNet Executive Group (C-EG) on behalf of the CFBLNet Senior Steering Group (C-SSG). The provisions of this and associated Publications shall govern the conduct of all business performed by the CFBLNet Participants, subject to their respective laws and military regulations.

105. The Security Working Group (SWG) is the technical body, comprised of appropriate technical security and accreditation experts from the Mission Partners, which supports the security governance process for the CFBLNet on behalf of the C-EG. The terms of reference and responsibilities of the SWG are described within Annex A, Terms of Reference.

Amendments

106. Annex C may be amended when the SWG determines that there is an identified requirement or technical change. The SWG Chairman will propose the text of the amendment to the SWG members for endorsement. Once the SWG members have endorsed the amendment, it will be submitted via the document management process as controlled by the Information Management Working Group (IMWG) for C-EG approval. Upon approval by the C-EG, the Secretariat will re-issue a new version of Annex C.

Effective Date

107. The current version of CFBLNet Pub 1, Annex C is effective upon the latest approval by the C-EG.

CHAPTER 2 – SECURITY OF INFORMATION

Infrastructure and Mode of Operation

201. The CFBLNet consists of the following components:

a. Backbone infrastructure (BLACKBONE): A common, closed, **Unclassified** routed IP V4/V6 network layer implemented using a mixture of both serial, ATM and IP bearer networks. Its primary purpose is to transport encrypted traffic throughout the network. The level and type of network services available within this component will be the minimal required to; support the interconnection of multiple enclaves as agreed to by all Core Mission Partners (CMPs), and Guest Mission Partners (GMPs).

b. CFBLNet Unclassified Enclave (CUE): A permanent routed IP V4/V6 enclave operating over the BLACKBONE and for a period of time over IP bearer network infrastructures. It will operate at the **Unclassified, Non Releasable to Internet Releasable to CMPs and to Guest Mission Partners (GMPs)** as directed by the C-EG. It must be noted that the CUE cannot be connected to any classified domains (though it may support any number of 'dummy' domains).

c. Temporary Enclaves: An enclave created for a finite period to support the execution of specific Initiatives and operating over the BLACKBONE and for a period of time over IP bearer network infrastructures. The level of classification and release caveats used within these enclaves will be determined by the Initiative requirements. The coordination and provision of all network services within a specific temporary enclave will be the responsibility of the Initiative sponsor.

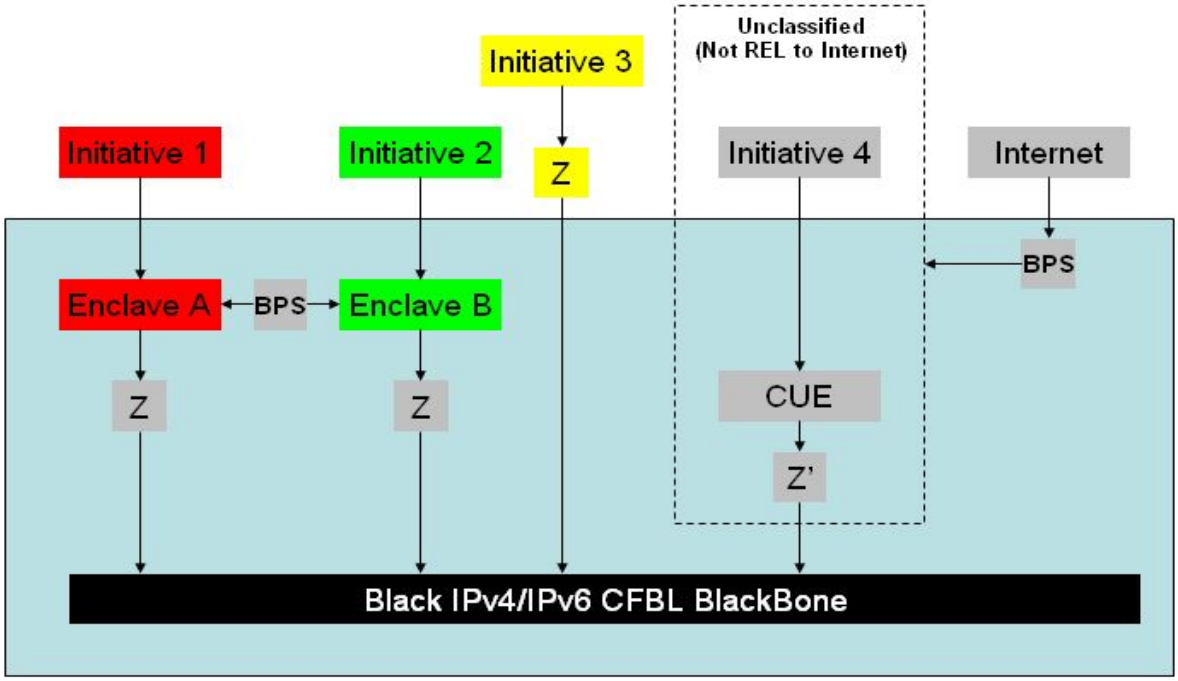

Figure C-1. CFBLNet Architecture Logical view

Cryptographic Separation

202. CFBLNet enclaves are protected by appropriate and approved encryption devices and border protection systems (BPS) for the assurance, as required, of information up to and including the classification level of TOP SECRET (TS). SECRET and TS Enclaves shall be cryptographically separated from other enclaves by Type 1 / NATO-approved products.

Classification of Information

203. CFBLNet enclaves permit handling, storage and transport of information classified up to and including TS. CFBLNet data shall be labeled with a releasability caveat determined by the Initiative accreditation, as specified in the CFBLNet Initiative Information Package (CIIP).

204. CFBLNet CMPs and GMPs users shall hold an appropriate security clearance valid for the duration of the authorized access and have a need to know. Separation of information domains on the network is achieved through technical and/or procedural means, to enforce the principle of "need to know" as well as 'need to share' as governed by the Initiative.

205. Each of the participating nations and NATO has their own way of protectively marking information for CFBLNet release. The following are samples of protective marking/security caveats and are equivalent to 'RELEASABLE to AUSCANZUKUS and NATO':

a. Australia: RELEASABLE to AUSCANZUKUS and NATO
b. Canada: RELEASABLE to AUSCANZUKUS and NATO
c. New Zealand: RELEASABLE to AUSCANZUKUS and NATO
d. United Kingdom: RELEASABLE to AUSCANZUKUS and NATO
e. United States: RELEASABLE to AUSCANZUKUS and NATO
f. NATO: NATO UNCLASSIFIED RELEASABLE to AUSCANZUKUS
g. National: RELEASABLE to AUSCANZUKUS and NATO
h. ISAF related: NATO SECRET REL ISAF or ISAF SECRET (example)

206. CFBLNet can use subsets of the above caveats for individual Initiatives as appropriate.

207. Appendix 3 provides guidance on how to classify information related to the conduct of Initiatives on CFBLNet.

Information release between CMPs and GMPs

208. Release of CFBLNet-related information from one CMP/GMP to another CMP/GMP falls, by default, under one of the following documents:

a. CFBLNet Technical Arrangement;
b. 5 eyes Memorandum Of Understanding 'CJM3IEM' managed by the CCEB;
c. NATO Security Agreements.

GMPs

209. The procedure on how to sponsor GMP is described in Annex F, GMP Sponsorship Processing.

Handling of Commercial Information

210. Commercial and Non-Military agencies/companies who are CMP/GMP sponsored to connect must adhere to National/Organizational Military Security and Installation standards. Commercial and Non-Military agencies/companies installation need to be isolated/protected from other networks based on the aforementioned standards.

211. Each nation/organization has a different caveat for protecting commercial information, listed below are examples of the national/organizational caveats for protecting commercially sensitive information. Any information marked with the caveats below shall not be shared with other commercial parties and Initiatives without the written permission of the originating party.

a. Australia – COMMERCIAL-IN-CONFIDENCE
b. Canada – PROTECTED (Commercial in Confidence)
c. New Zealand – COMMERCIAL-IN-CONFIDENCE
d. United Kingdom – OFFICIAL SENSITIVE COMMERCIAL
e. United States – Unclassified Proprietary
f. Nation – Unclassified Proprietary or others as appropriate
g. NATO – Commercial-in-Confidence

CHAPTER 3 – SECURITY ASPECTS OF NETWORK ARCHITECTURE

Network Architecture

301. Detailed descriptions of the CFBLNet Communications and Information System (CIS) architecture can be obtained from the CFBLNet Pub1, Annex D.

Initiative Architecture

302. The CIIP will contain all the details of the security architecture for a given Initiative (see Chapter 4 on the security aspects of the CIIP). The SWG considers the Initiative proposal based on the most recent version of its CIIP and any other details provided through the CMP/GMP Lead Representative (CLR/GLR) or Initiative Lead. The CFBLNet SWG is required to advise the C-EG on the security architecture of the proposed Initiative.

303. The CFBLNet SWG may require Initiatives to stand up and maintain an Initiative Chaired Security WG if the perceived level of risk requires it. This selection will be done on a case by case basis depending upon one or more of the following criteria:

a. Multiple domains or enclaves;
b. Cross domain solutions;
c. Multiple classification and/or releasability;
d. Long term Initiatives.

Generic Security Requirements and Interconnection of Enclaves

304. Initiative Requirement. The requirement for interconnecting an enclave to another enclave shall be formally stated by the requesting CMP/GMP. The Initiative requirement shall identify, as a minimum, the classification and releasability of the information to be exchanged.

305. Security Requirement. Prior to implementation of the interconnection, the security requirement shall be established and documented in accordance with the requirements of the CMP sponsor Accreditation Authorities.

306. Risk Assessment/Risk Management. The interconnection shall be subject to the requirements of the CMP/GMP Accreditation Authorities for risk assessment and risk management; and shall be subject to on-going risk management/monitoring.

307. Security Vulnerability Testing. Security vulnerability testing by the lead CMP/GMP for the Initiative is to verify that interface devices, services and procedures are correctly configured and implemented.

308. Security Education and Awareness. The Initiative users, system and security administrators shall be provided with on-going security education to maintain a high level of security awareness of the technical and non-technical security measures in place for the protection of information and inter-networking services and enclave assets.

309. Accreditation. The interconnection shall be approved by the C-EG and accredited by the appropriate CMP/GMP Accreditation Authorities endorsed by the Multinational Security

Accreditation Board (MSAB), or a minimum to have an Interim Approval to Operate, IATO (see Chapter 5).

310. Disconnection of Service. Site and Initiative security accreditation must remain current or services will be disconnected. It is the CMP/GMP Accreditation Authority responsibility to disconnect the CMP/GMP site under their responsibility when the sites are no longer accredited.

311. Mobile/Cellular. Personal Electronic Devices (PED) using wireless, 3G and Bluetooth will have to adhere to the National policy at the user location when connecting to CFBLNet domains.

Interconnection Scenarios

312. The diagram below illustrates the various interconnection scenarios for which Boundary Protection and encryption requirements have been defined by the SWG and endorsed by the MSAB. Initiatives relying on other interconnection scenarios shall refer back to the SWG who will provide further guidance on a case by case basis.

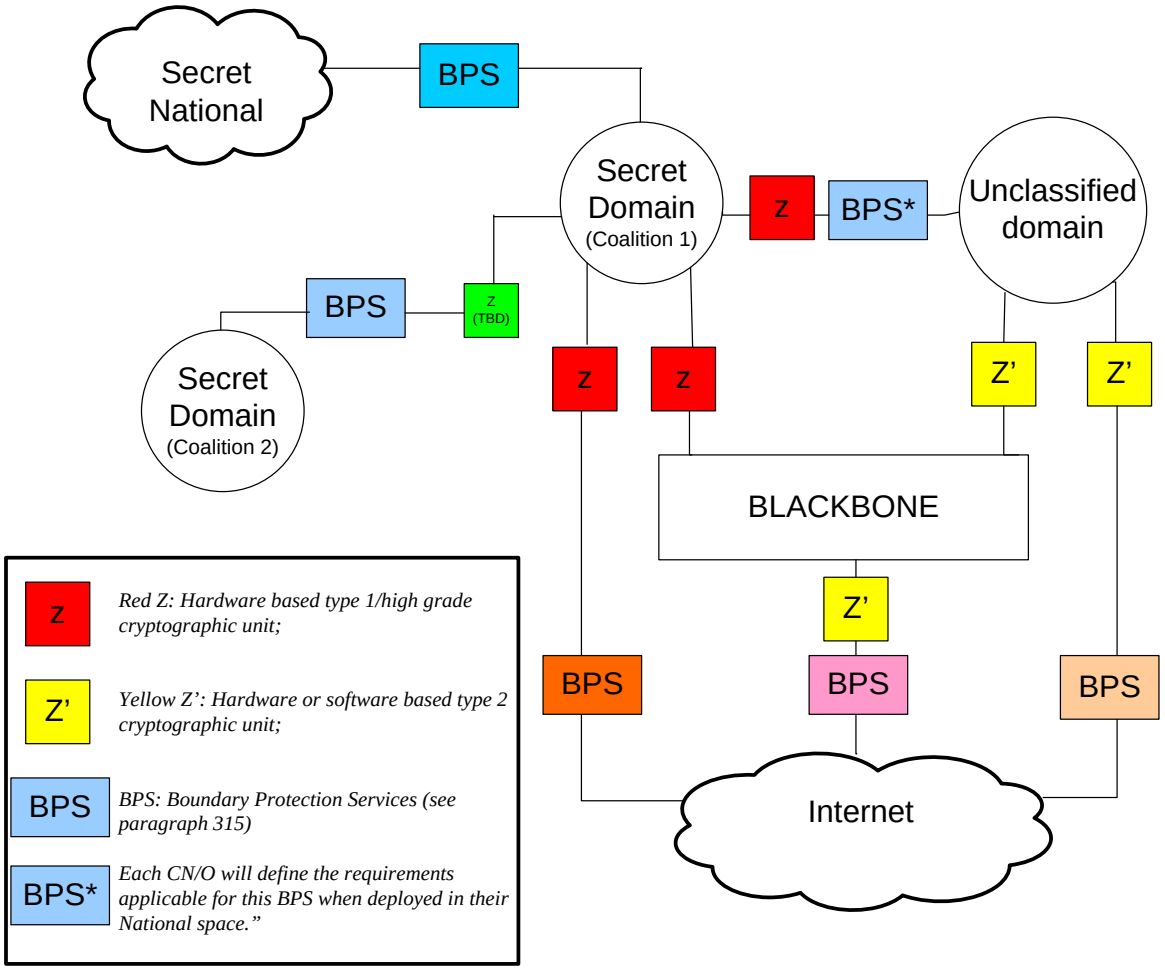

Figure C.2: Interconnection scenarios for Initiatives running over the CFBLNet

313. Boundary Protection Services (BPS) is a generic concept that provides security services (through tools, processes and procedures) needed whenever an enclave interfaces with another. These services can be provided by any of a number of tools and devices, such as firewalls, encryption devices, routers, filters, guards, proxy servers, etc., either alone or in combination. The requirements for BPSs are addressed in each interconnection architecture.

BPS Requirements for Connections to the Internet

314. SECRET and TS enclaves cannot be directly connected to the internet. However, indirect connection to the Internet can be considered if this connection is compliant with the connecting Nation's policy and all participating Nations of a given Initiative are informed of and endorse this connection.

315. The minimum Boundary Protection Requirements for connecting an UNCLASSIFIED Network to the Internet are:

a. a Common Criteria EAL-2 evaluated (or National equivalent) firewall;
b. an Intrusion Detection System (IDS) tool (desirable though not required for the CUE);
c. a malicious content checker updated at least weekly or on CERT recommendation.

316. The minimum Boundary Protection Requirements for connecting the BLACKBONE to the Internet is:

a. Filtering router with Access Control List (which can not be remotely managed through the Internet).

BPS Requirements for Connections of Domains or Enclaves of Different Releasability

317. Initiatives with a requirement to connect domains or enclaves of different releasability shall refer back to the MSAB Reps of the CMP/GMPs involved in the Initiative, who will provide further guidance on a case by case basis. The CFBLNet SWG should be fully engaged at the early stages of the discussion and will provide recommendations to the MSAB.

BPS Requirements for Back-End Connections to National Systems

318. The minimum Boundary Protection Requirements for connecting a SECRET Network to a National SECRET System are:

a. minimum Common Criteria EAL 4 (or National equivalent) Guard[1]

[1] A classified CFBLNet enclave may be connected to a dummy domain by an unevaluated BPS, controlled by that member CMP/GMP. The dummy domain needs to be maintained at the appropriate security protection level for the classification of the information being exchanged.

b. an Intrusion Detection System (IDS) tool;
c. malicious content checker updated at least weekly or on CERT recommendation; and
d. a keyword search tool.

Encryption/Tunnelling Requirements

319. The Minimum Encryption/Tunneling Requirements for sending Unclassified information from an Unclassified Domain through the Blackbone or the Internet are:

a. a hardware or software based type 2 cryptographic unit (Z') with the following features:
   i. 128 AES or 1024 RSA algorithm;
   ii. US Federal Information Processing Standards (FIPS) 140-2 or Common Criteria EAL2 (or national equivalent) evaluated;
   iii. IPv6 compatible (desirable)
b. cryptographic keys shall be distributed according to an agreed and published key management plan. The key material should be unique to each Community of Interest (COI) that requires protection/isolation from other initiatives.

320. The Minimum Encryption/Tunneling Requirements for sending Classified information from a SECRET Domain through an Unclassified domain, the Blackbone or the Internet are:

a. a hardware based type 1/high grade cryptographic unit (Z) with the following feature: National evaluation and/or approval to use the cryptographic unit to encrypt classified information (up to the required level);
b. cryptographic keys shall be distributed according to national policies and key management plan.

Classified Enclaves Interconnection Requirements

321. Other initiatives with a requirement to send classified information from a SECRET Domain through another SECRET Domain but with a different releasability scheme shall refer back to the MSAB Reps of the CMPs/GMPs involved in this Initiative who will provide further guidance on a case by case basis. The CFBLNet SWG should be fully engaged at the early stages of the discussion and will provide recommendations to the MSAB.

Use of Unevaluated/Unapproved Devices

322. All cross-domain interconnections using unevaluated or unapproved devices require a security risk assessment compliant with International Standards (e.g. ISO,17799, ISO27001, ISO27002, NIST800-30) to be conducted by the 'cross-domain interconnection sponsor'. The following process is to occur:

a. a summary of the risk assessment is to be provided by the appropriate CLR/GLR to the Secretariat for distribution to the SWG members to determine the overall risk to the CFBLNet community;

b. the appropriate CMP/GMP Accreditation Authority is to provide the risk assessment summary to the appropriate MSAB rep;
c. the respective MSAB rep provides the risk assessment summary to the MSAB for endorsement; and
d. the recommendations by the SWG and MSAB are to be provided to the CFBLNet Secretariat for the C-EG to evaluate.

CHAPTER 4 – SECURITY ASPECTS OF THE CIIP

Introduction

401. The SWG considers an Initiative proposal based on its published CIIP and any other details provided. The CIIP addresses the security aspects of the Initiative and, for that reason, is a major input for the SWG to make a recommendation to the C-EG for approval for the Initiative to execute.

Legal Framework

402. One important thing, often overlooked when completing the security portion of the CIIP, is the identification of the Memorandum of Agreement (MOA) or Information Sharing Agreement (ISA) covering the exchange of classified data between all participating CMPs and GMPs in each domain or enclave used by the Initiative. Attention: the issue of releasability, exploitation and further reuse of classified Initiative data is not covered by the CFBLNet Technical Arrangement and, from a legal point of view, needs to be addressed formally before the Initiative is able to proceed. An MOA/ISA needs to be in place and effective for the complete duration of the Initiative it is covering.

Interconnections

403. The security portion of the CIIP is mandatory to provide an accurate picture of all the interconnected enclaves and cross domain boundary/networks to be used by the Initiative. Interconnection of a CFBLNet enclave with a non-CFBLNet enclave poses additional threats against the confidentiality, integrity and availability of CFBLNet information as well as the integrity and availability of the CFBLNet as a whole. Aspects of concerns can be:

a. the increased number of users of the enclaves;
b. all backend connections/systems that may be unknown to the system/security managers/data owners of the enclaves;
c. connections to the Internet;
d. alteration of the security posture of members in the enclave;
e. introduction of unmanaged risks to the community.

404. The SWG will assess the level of risk associated to such interconnections and will take into consideration factors like:

a. the inter-networking services allowed across the interconnection;
b. the Evaluation Assurance Level (EAL) of the security-enforcing components of the CFBLNet enclave Boundary Protection Services (BPS);
c. the operation and maintenance of the interconnection.

Timelines

405. Since some security requirements (such as those derived from Cross-Domain architectures or scenarios involving new Mission Partners) can have a major impact on the Initiative network architecture, Initiative Lead are encouraged to liaise with the SWG as soon as possible in the CIIP drafting process so as to defuse any issue related to security (that could be raised later during the formal CIIP review).

CHAPTER 5 – SECURITY ACCREDITATION

Introduction

501. Accreditation is defined as a formal declaration by a CMP/GMP Accreditation Authority that a CIS or network is approved to operate in a particular security mode at a defined classification level approved to operate at appropriate accreditation standards using a prescribed set of safeguards at an acceptable level of risk.

502. Sites must be accredited before they can be considered operational CFBLNet Sites.

503. Initiative must also be accredited for a given site in order to use the infrastructure of this site. The following certificates are being used to indicate the accreditation status of Sites and Initiatives:

a. Site-National Accreditation Endorsement Certificate (S-NAEC). This certifies that a site has met the security requirements for a baseline of equipment that is used to transport information between CFBLNet member sites. The time period of a valid S-NAEC is controlled by each CMP/GMP Accreditation Authority. All S-NAEC's will be issued by the MSAB. It must be noted that the CUE requires its own accreditation (that cannot exceed the CFBLNet Site Accreditation timeframe).
b. Initiative-National Accreditation Endorsement Certificate (I-NAEC). This certificate in conjunction with an S-NAEC permits a site to participate in a CFBLNet Initiative. The maximum time an I-NEAC is valid for is one year.
c. The above documents will be issued by each nation's respective MSAB rep.

Security Accreditation Authorities

504. The authorities involved in the process for gaining accreditation and authority to operate are:

a. CMP/GMP Accreditation Authority
b. MSAB
c. CFBLNet Secretariat (for record purpose only)

Role of the CMP/GMP Accreditation Authority

505. The CMP/GMP Accreditation Authority is responsible for the accreditation of all infrastructure and services located behind its CMP/GMP boundary or POP.

506. When a site has achieved CMP/GMP accreditation, the CMP/GMP Accreditation Authority makes a formal declaration of this to their MSAB representative and requests the site be certified as an accredited CFBLNet site. This formal declaration takes the form dictated by national or organizational policies.

507. The CMP/GMP is also responsible for ensuring that each proposed Initiative has met similar standards for accreditation, and makes a formal representation of such to their MSAB representative. Any and all security issues raised by the MSAB representative must be

satisfactorily addressed by the CMP/GMP Accreditation Authority before the MSAB member will further process the site or Initiative request.

Role of the MSAB

508. The MSAB is the security accreditation endorsement authority for activities executing within the CFBLNet CIS.

509. The MSAB Chair coordinates the completed Site or Initiative National Accreditation Endorsement Certificates (S-NAEC or I-NAEC) from the CMP/GMP Accreditation Authorities, via the relevant MSAB representative.

510. A Statement of Conformity (SOC) will be prepared as required by each GMP participant in a project or Initiative by that nation/organization and distributed to the appropriate sponsoring CMP MSAB representative (or MSAB Chair) as formal acknowledgement that an agreed upon formal accreditation process has been followed. The Initiative or system will be accredited, physically labeled and protected to the level appropriate classification of information stored, processed or communicated on that Initiative or system by that GMP participant.

511. If a specific Initiative utilizing the CFBLNet requires further confirmation of national accreditation status, it will be the responsibility of the Initiative management to solicit the required confirmation from the MSAB.

Role of the Secretariat

512. The Secretariat maintains copies of the official MSAB records (NAECs) of all accredited components (Sites, Enclaves and Initiatives) of the CFBLNet.

513. The CFBLNet Secretariat can access an up-to-date copy of the CFBLNet related MSAB records (NAECs) to advise, as appropriate, the CLR(s)/GLR(s) and ensure that there is no lapse in the accreditation of CMP/GMP CFBLNet Sites. Any question(s) regarding S and/or I-NEAC(s) should be addressed through the National / Organizational MSAB Rep. The MSAB is the sole authority on National and Organizational Site and Initiative security accreditation matters.

Accreditation Procedures

Overview

514. The accreditation process can be seen as a process parallel but independent of the CIIP approval process (which is described in Annex B of Publication 1). All requirements relating to accreditation, including Core and Guest Mission Partners are addressed in the MSAB accreditation policy and work processes which are defined in the MSAB Terms of Reference (TOR).

515. In summary, Site or Initiative accreditations are first issued by CMP/GMP Accreditation Authority, who submits the request and accreditation information to his MSAB representative. When all CMP/GMP security requirements have been met, the MSAB member generates a Site National Accreditation Endorsement Certificate (S-NAEC) and/or an Initiative National

Accreditation Endorsement Certificate (I-NAEC), which is submitted to the MSAB Chair, other MSAB members and for the record, the Security Coordinator of the Secretariat.

516. In some cases the CMP/GMP Accreditation Authorities for Unclassified Initiative is different than for Classified Initiative. This might have an effect on the CMP/GMP accreditation timelines.

Site Accreditation

517. In order for an Initiative to be conducted, at least two approved involved sites must have their Site and Initiative Accreditations with MSAB certificates issued. Other sites will be able to join later on as their Site and Initiative NAECS are endorsed by the MSAB.

518. The Site Accreditation process starts with the CMP/GMP Site Security Authority checking the implementation of the security requirements applicable to the connection of the Site infrastructure to the CFBLNet.

519. When the Site/Local Accreditation Authority has determined that the site has met the specified security requirements, the Site Accreditation package is sent to the CMP/GMP Accreditation Authority for approval.

520. When the CMP/GMP Accreditation Authority has determined that the Site has been correctly accredited to CMP/GMP and CFBLNet standards the accreditation package is submitted to the CMP/GMP MSAB Representative for Endorsement. The MSAB Rep then determines whether the Site has been accredited in a manner which satisfies CFBLNet requirements.

521. When the CMP/GMP MSAB Rep has endorsed the site accreditation, the S-NAEC (see NAEC template at Appendix 2) is competed and notification is made to the MSAB Chair, the other MSAB members and the Secretariat that the site has approval to operate.

Lapse in the Renewal of S-NAECs

522. If an S-NAEC expires during the conduct of an Initiative, then the Site has to immediately stop its support to this Initiative. However, this does not stop the other involved sites from supporting the same Initiative.

523. It is the responsibility of the CLR/GLR to prevent this situation from happening by ensuring that there is no lapse in the renewal of the accreditation of his National/Organizational CFBLNet Site(s).

524. The CFBLNet Secretariat will send the CLR/GLR a reminder two months before the expiration of an S-NAEC.

525. Eventually, a warning will be sent by the CFBLNet Secretariat to the CLR/GLR four weeks before the expiration of an S-NAEC to confirm the active/inactive status of the site.

Initiative Accreditation

526. The Initiative Accreditation process starts with the CMP/GMP Security Authority checking the implementation of the security requirements applicable to the connection of the systems supporting a given Initiative to one or more approved CFBLNet Sites.

527. When the CMP/GMP Accreditation Authority has determined that the Initiative correctly implements the CMP/GMP and CFBLNet security standards, the accreditation package is submitted to the CMP/GMP MSAB Representative for Endorsement. The MSAB Rep then determines whether the Initiative has been accredited in a manner which satisfies CFBLNet requirements.

528. When the CMP/GMP MSAB Rep has endorsed the Initiative accreditation the I-NAEC (see NAEC template at Appendix 2) is completed and notification is made to the MSAB Chair, the other MSAB members and the Secretariat that the Initiative on that site has approval to operate. **In order to allow timely distribution of documentation, I-NAEC must be issued at least three days before the start of the Initiative. Failure to meet this requirement could negatively impact participation in the rest of the Initiative.**

529. The decision on whether an Initiative already accredited requires a new accreditation depends upon the software and hardware configuration / changes that will have occurred since the last accreditation. The decision rests with the Site/Local Accreditation Authority in co-ordination with the Initiative Lead and Lead CMP/GMP Accreditation Authority. Where no accreditation is required, the Site/Local Accreditation Authority will notify the Initiative Lead, who will inform the National/Organizational Leads and CFBLNet Secretariat Coordinator. Initiative Accreditation procedures are the same for classified and unclassified enclaves.

CHAPTER 6 – COMMUNICATIONS AND INFORMATION SYSTEMS (CIS) SECURITY

Introduction

601. The objective of this section is to establish the basic principles for CMP/GMP to follow in order to achieve a coordinated approach to CIS security.

602. In the context of this document, CIS security is defined as '*The application of security measures for the protection of communication, information and other electronic systems, and the information that is stored, processed or transmitted in these systems with respect to confidentiality, integrity, availability, authentication and non-repudiation'*.

603. Each CMP/GMP will have its own security policy/strategy and will maintain flexibility in how to respond to different types of security incidents.

604. In the rest of this section, CFBLNet assets are defined as hardware or software assets supporting the CFBLNet mission and services (at the infrastructure or Initiative level).

Principles

605. It is advised that each CMP/GMP implements a CIS Security strategy addressing at least the following principles:

a. Education training and awareness: Each CMP/GMP should ensure that security practices are regularly exercised for all roles within CFBLNet (e.g. end user, administrators).
b. Accountability: Each CMP/GMP should ensure that only authorized users that have signed the relevant Security Operating Procedures have access to CFBLNet assets.
c. Resilience: Each CMP/GMP should ensure that the security design and configuration of CFBLNet assets under their responsibility can withstand security incidents and provide appropriate continuity of service.
d. Detection: Each CMP/GMP should have the ability to detect malicious activity on a network enclave under their responsibility by collecting sensor information.
e. Response: Each CMP/GMP should have the ability to react to any malicious activity detected on CFBLNet assets under their responsibility.
f. Recovery: Each CMP/GMP should have the ability to recover from any adverse event with appropriate restore time. Recovery activities should include verification of the integrity of CFBLNet assets and ensure that no loss of confidentiality resulted.
g. Security Event Sharing: Timely information sharing is critical to enabling shared situational awareness between CMP/GMP as well as early warning of security incidents (see appendix 4 on CFBLNet Incident Reporting).

606. It is advised that, whenever possible and relevant, each CMP/GMP takes advantage of initiatives run on CFBLNet to exercise the workflow of security incident reporting described in Appendix 4.