

COMBINED FEDERATED BATTLE LABORATORIES NETWORK (CFBLNet)



Guide

Version 3.0

March 2025

DOCUMENT CONTROL

Date	Agent Type	Agent Name	Event Type	Event Description
Sep 2017	C-EG Chair	Lt Col J. Trepka	Review, Approve	CFBLNet Guide, Version 1.0
Oct 2019	C-EG Chair	Maj J.D Williams	Review, Approve	CFBLNet Guide, Version 2.0
Mar 2025	C-EG Chair	N Kerschl	Review, Approve	CFBLNet Guide, Version 3.0

APPROVAL

The Guide is hereby approved by the C-EG.



Nicholas Kerschl

USA Joint Staff/J6

USA DoD C-EG Representative and Chair

With concurrence and endorsement from:

LTCOL Andrew Flook

CCEB Washington Staff

CCEB C-EG Representative

DR Michael Rudack

NATO Communications and Information Agency

NATO C-EG Representative

INFORMATION AND CONTACTS

Information can be found on the following web-site:

https://community.apan.org/wg/cfblnet/cfblnet_public/

Further information about CFBLNet or the contact details of your Country Lead Representative (CLR) can be found at:

SAF.CFBLNet.Secretariat@us.af.mil

Please include your name, organization, country and a brief explanation for your request.

TABLE OF CONTENTS

CHAPTER 1 OVERVIEW	1
1.1 DESCRIPTION	1
1.2 MANAGEMENT STRUCTURE.....	2
1.3 NETWORK ARCHITECTURE	2
1.4 INITIATIVES.....	2
1.5 SECURITY.....	2
1.6 CHANGE PROCESS	2
CHAPTER 2 MANAGEMENT STRUCTURE	3
2.1 CFBLNET SENIOR STEERING GROUP (C-SSG).....	3
2.2 CFBLNET EXECUTIVE GROUP (C-EG).....	3
2.3 CFBLNET SECRETARIAT	3
2.4 CFBLNET MISSION PARTNER LEAD REPRESENTATIVE.....	4
2.5 MULTINATIONAL SECURITY ACCREDITATION BOARD (MSAB)	4
2.6 SECURITY WORKING GROUP (SWG)	4
2.7 NETWORK WORKING GROUP (NWG)	4
2.8 INITIATIVES WORKING GROUP (IWG)	4
2.9 INFORMATION MANAGEMENT WORKING GROUP (IMWG).....	4
2.10 ATTENDANCE AT MEETINGS	4
2.11 TOOLS.....	5
CHAPTER 3 NETWORK OPERATIONS AND SERVICES.....	6
3.1 INFRASTRUCTURE	6
3.2 CFBLNET SITES.....	6
3.3 NETWORK SERVICES OVERVIEW	6
3.4 CORE NETWORK SERVICES	6
CHAPTER 4 INITIATIVES.....	7
4.1 CFBLNET INITIATIVES	7
4.2 INITIATIVE PARTICIPATION.....	7
CHAPTER 5 CFBLNET SECURITY AND INFORMATION ASSURANCE.....	8
5.1 OVERVIEW	8
5.2 SECURITY PROCESS	8
5.3 PERSONNEL SECURITY	8
ANNEX A FREQUENTLY ASKED QUESTIONS (FAQ) S	A1
ANNEX B GLOSSARY AND ABBREVIATIONS	B1

CHAPTER 1 Overview

This Guide is intended to give prospective participants an overview of the Combined Federated Battle Laboratories Network (CFBLNet) and the practices and procedures used within this community. A companion document, “The Manual,” provides additional detail regarding the conduct of all activities performed on the infrastructure or by the CFBLNet community. In addition, the CFBLNet Technical Arrangement (Charter) defines the operation and conduct of the CFBLNet mission.

1.1 Description

The CFBLNet is a voluntary association of Core Mission Partners (CMP) comprising nations from North Atlantic Treaty Organisation (NATO), the Combined Communications-Electronics Board (CCEB) and the United States of America (USA). NATO represents its organisational interests and the interests of Mission Partners (MPs) who are members of NATO, except for CAN, GBR and the USA. The CCEB represents its organisational interests and the interests of MPs who are members of CCEB, AUS, CAN, GBR and NZL. The USA represents itself. For the purposes of the CFBLNet CMPs belong to one of the three entities (USA, NATO and CCEB). Other nations are encouraged to participate in events by becoming a Guest Mission Partner (GMP) through sponsorship by a CMP. Figure 1 shows the current MPs.

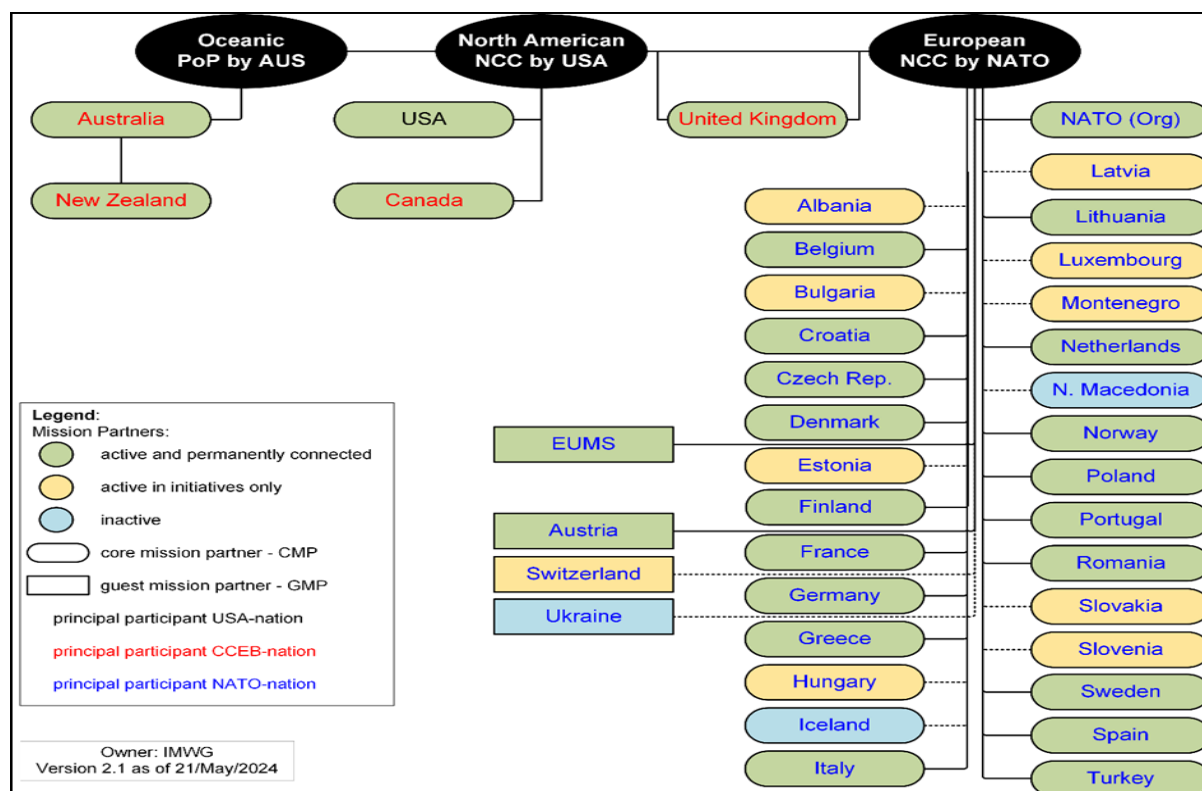


Figure 1 - Countries with CFBLNet partnership

CFBLNet provides the infrastructure of choice for Research, Development, Trials, And Assessment (RDT&A), as well as Training and Exercise (T&E), or cyber activities, which enables MPs to field comprehensive operational Command, Control, Communication, Computers, Cyber, Intelligence, Surveillance and Reconnaissance (C5ISR) and training capabilities.

CFBLNet does not support operational usage or information exchanges.

The changing nature of actual and future warfare demands that CFBLNet be capable of evolving to support the integration of all MPs involved across the spectrum of operations, regardless if they are nations or organisations (NATO in the context of CFBLNet is seen as a MP).

Each MP is responsible for managing and supporting its own national infrastructure, which collectively form the CFBLNet. This may include resources to run applications, analytic tools, security devices and communications necessary to conduct initiatives. The US Air Force Mission Partner Capability Office (MPCO) in coordination with the MPs will centrally coordinate network management.

1.2 Management structure

The CFBLNet community is staffed at flag level who determine the strategy for current and future years. The strategy is then implemented by a guiding executive group and various working groups with national representation. Our community consists of stakeholders mainly from government but also academia and industry. CFBLNet will continuously target stakeholder engagement to remain the infrastructure of choice for RDT&A, training, exercises and cyber activities. The whole process is assisted by a secretariat based in the USA. Chapter 2 provides greater detail.

1.3 Network architecture

CFBLNet is a closed wide area communications network (using persistent or temporary enclaves) and utilising practises and procedures in order to deliver a robust and accredited network operating at the relevant security classification and releasability. The CFBLNet consists of distributed and integrated network architectures, based on an Internet Protocol (IP) backbone (Blackbone) network.

The CFBLNet has two Network Control Centres (NCCs) located in the USA and Europe with an access point in Australia. The NCCs are available 24/7, however engineering support may not be available outside regional operational hours.

1.4 Initiatives

An initiative encompasses any activity that requires the use of a network for a single or a number of test-events with a given participation. All initiatives require the submission of a CFBLNet Initiative Information Package (CIIP). An initiative is usually conducted in a single enclave comprising all infrastructure components with the same classification and the same releasability.

1.5 Security

Each initiative participant is responsible for implementing CFBLNet security management policies and procedures in conjunction with their own national/organisational security policy.

1.6 Change process

Potential changes are submitted to the Change Manager (CM) which is coordinated by the Information Management Working Group (IMWG). After consideration by the relevant persons or working groups if changes are required this will then be sent to the C-EG for approval.

CHAPTER 2 Management Structure

The CFBLNet organisational hierarchy is shown in Figure 2.

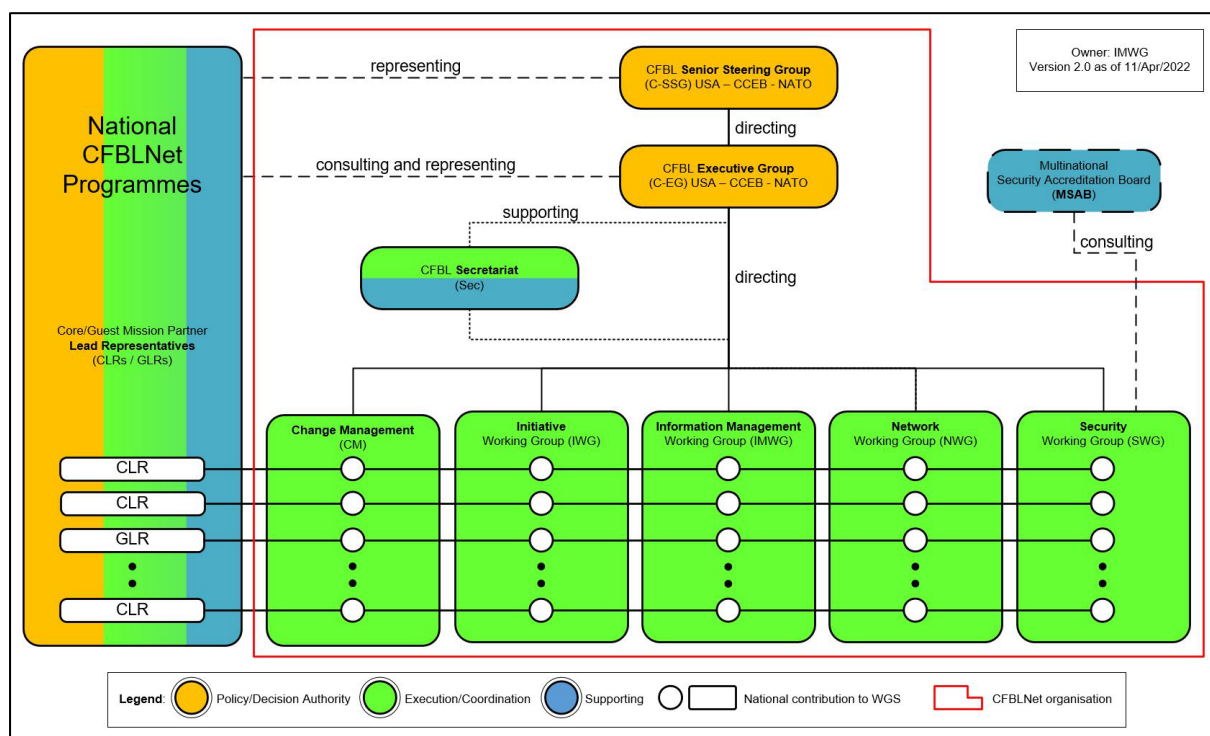


Figure 2 – Organisational hierarchy

2.1 CFBLNet Senior Steering Group (C-SSG)

The C-SSG is a flag-level group that provides overall direction for CFBLNet activities. The C-SSG includes one representative from the USA, CCEB and NATO.

The C-SSG provides leadership and executive oversight on all CFBLNet matters. It reviews CFBLNet procedures, receives reports on CFBLNet activities, considers the general programme of proposed initiatives and directs improvements to the CFBLNet. It informs the CFBLNet community to provide network capabilities and services to the participating national and international organisations, responding to their requirements.

2.2 CFBLNet Executive Group (C-EG)

The C-EG is the executive body also consisting of one representative from the USA, the CCEB and NATO. They provide policy and decision-making on behalf of the C-SSG and are a staff level management group responsible for the determination of CFBLNet requirements and uses. The C-EG is the approving body for any initiative requested by the MPs for execution on CFBLNet and will direct the focus of stakeholder engagement. The US representative chairs this group.

2.3 CFBLNet Secretariat

The CFBLNet secretariat currently resourced by the USA is tasked to support administration of a number of CFBLNet activities. These duties include the managing of the public and closed user-group web-sites on APAN as well as the initiative matrix and the roster of all national representatives. The secretariat is responsible for initiating the monthly teleconferences of all the different groups as well as producing and distributing the minutes. Other duties also include

coordinating with the relevant hosting nation the face-to-face meetings of the CFBLNet community which are held annually CFBLNet Management Meeting (CMM) in April / May and the CFBLNet Engineering Meeting (CEM) held in October.

2.4 CFBLNet Mission partner lead representative

MPs are represented by the Core/Guest Lead Representatives (CLRs/GLRs - LR). The LR facilitates the participation of the MP in CFBLNet. They act as the single point of contact for their nation in regard to the usage of CFBLNet. A volunteer CLR is nominated to lead CLR/GLRs during CMM and CEM events. This position is not required to be ratified by the C-EG.

2.5 Multinational Security Accreditation Board (MSAB)

The MSAB is a multinational body that exists to facilitate and endorse the security accreditation of interconnected information systems. The MSAB provides a process of mutual recognition of security accreditation to ensure a holistic approach to the security of coalition information including those networks and enclaves established under the auspices of the CFBLNet.

2.6 Security Working Group (SWG)

The SWG is the CFBLNet working group consisting of MPs security representatives where security, cyber and information assurance issues for the CFBLNet are coordinated in order to support the execution of initiatives on the CFBLNet. A volunteer Subject Matter Expert (SME) is nominated to chair this group after ratification by the C-EG.

2.7 Network Working Group (NWG)

The NWG is the CFBLNet working group consisting of MPs network specialists by which centralised network engineering and system operations are coordinated in order to support the execution of initiatives on the CFBLNet. The NWG develops guidance provided to those engineers and technicians who request technical support for connectivity over the CFBLNet. A volunteer SME from the US is nominated and chairs this group after ratification by the C-EG.

2.8 Initiatives Working Group (IWG)

The IWG is the CFBLNet working group consisting of LRs by which the process of using the CFBLNet is governed throughout the whole process from the initial planning to the final reporting. On a weekly basis the IWG chair holds a teleconference with the secretariat to review the initiative matrix and any issues that may be arising. A volunteer is nominated to chair this group after ratification by the C-EG.

2.9 Information Management Working Group (IMWG)

The IMWG is the CFBLNet working group which manages the process of creating, developing and changing CFBLNet policy, guidance and advertising documentation, throughout a documents life cycle. A volunteer is nominated to chair this group after ratification by the C-EG.

2.10 Attendance at meetings

It is highly desirable that all MPs are represented at the monthly teleconference Working Groups (WGs) and participate in both the CFBLNet Management Meeting (CMM) and CFBLNet Engineering Meeting (CEM). The monthly WG's and annual meetings provide invaluable information for all MPs.

2.11 Tools

To assist in the running of CFBLNet, the Secretariat maintains and monitors a member only instance of SharePoint hosted via the All Partner Access Network (APAN) website. The APAN SharePoint instance provides a central platform for the Secretariat to provide governance information and coordinate CFBLNet initiatives on behalf of the CFBLNet community.

The Secretariat also maintains the public facing CFBLNet website (details at top of document).

CHAPTER 3 Network Operations and Services

3.1 Infrastructure

The CFBLNet infrastructure is a closed, wide area communications network linking MP infrastructures, collectively forming the CFBLNet. The wide area network (WAN) overview with indicative bandwidths is shown in Figure 3. MPs are responsible for providing connectivity between their national sites and their respective national Point of Presence (PoP) which will serve as their connection gateway to the CFBLNet.

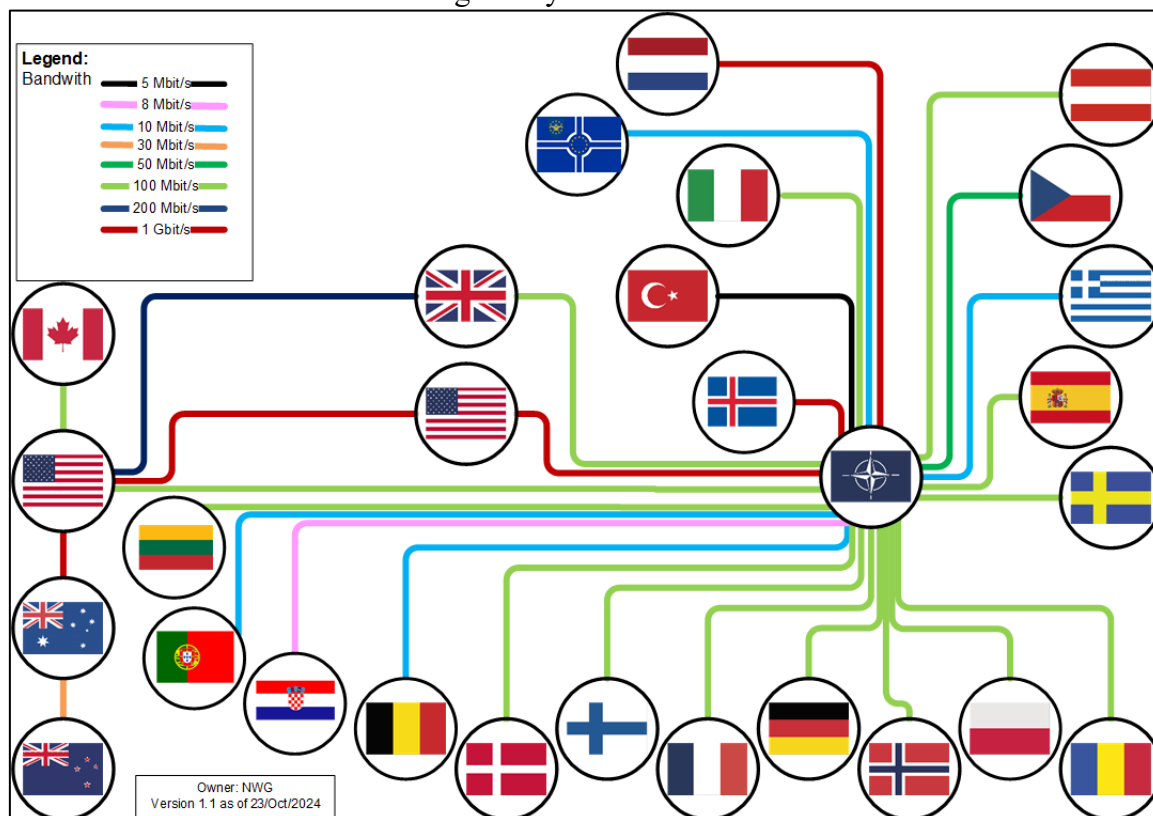


Figure 3 – Schematic CFBLNet WAN

3.2 CFBLNet sites

CFBLNet sites are those operational participant sites accredited through the CFBLNet security process. Each CLR will provide an up-to-date list of their sites twice a year on APAN.

The PoP is the CFBLNet site in each nation that provides supporting infrastructure and the connectivity to at least one of the NCCs and therefore to all other MPs.

3.3 Network services overview

Each MP maintains and operates agreed levels and types of network services for the CFBLNet permanent components to facilitate initiatives. These network services inter-operate with other MPs services to provide a collective network community.

3.4 Core network services

Core network services are robust, reliable and stable services, which have been developed and deployed on the CFBLNet permanent components to support initiatives. They are managed and supported by the MPs. Amongst others, they consist of domain name services (DNS), electronic mail (E-mail), network time protocol (NTP), IP telephony (VoIP) and web services i.e. hypertext transfer protocol (HTTP) and hypertext transfer protocol secure (HTTPS).

CHAPTER 4 Initiatives

4.1 CFBLNet initiatives

An initiative is a single or a series of test-events conducted between two or more MPs. For each initiative, one LR is responsible and in collaboration with the secretariat collects all the necessary data in the CFBLNet productivity tool (CPT). An extract of this information in one document is called a CIIP. Each relevant WG will endorse their area of the CIIP prior to submission to the secretariat and then approval from the C-EG prior to an initiative commencing. Figure 4 shows a simplified initiative workflow process for a CIIP including security aspects.

Information held in a CIIP includes scheduling, aim, points of contact (PoCs), classification, releasability, information on sites, end systems, security measures and network connectivity as well as bandwidth-usage etc.

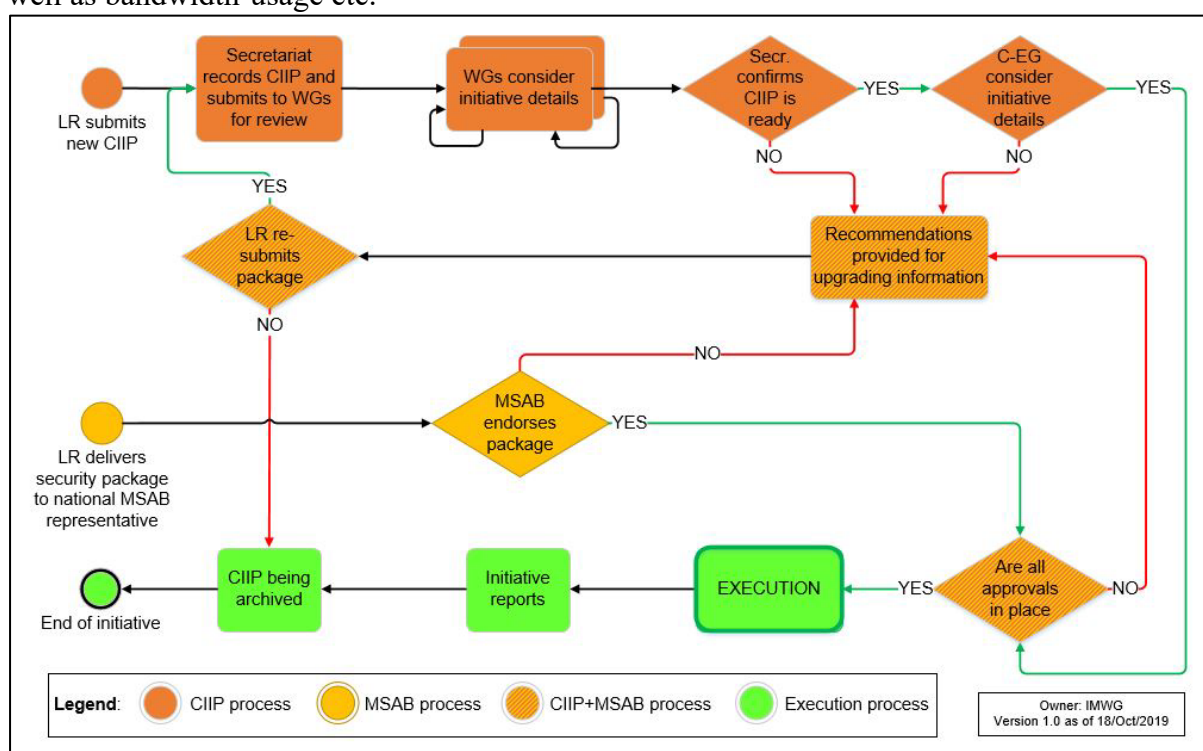


Figure 4 – Simplified initiative workflow

4.2 Initiative participation

An initiative can be originated by any MP. The time taken to approve an initiative will depend on the complexity both from an engineering and security perspective. An initiative may be approved in less than 21 calendar days whilst a more complex one may take in excess of 90 calendar days. Participants involved in initiatives are responsible for bearing their own costs to become involved. An initiative running to schedule can last for up to one year, however it may be terminated at any time by the unanimous consent of all participants.

When completing a CIIP ensure that the relevant agreements covering the exchange of data between all participating MPs in the initiative is addressed.

CHAPTER 5 CFBLNet Security and Information Assurance

5.1 Overview

The CFBLNet has processes in place for certification and accreditation of sites and initiatives. Information assurance procedures will be conducted in accordance with CFBLNet and national information systems accreditation policies, directives and processes. Failure to comply has the potential to damage the overall security posture of the network.

5.2 Security process

The SWG considers an initiative proposal containing the security level and the releasability which can be found in the CIIP. The security portion of the CIIP is mandated to provide an accurate picture of all security aspects including the interconnection of enclaves to be used by the initiative. This may be achieved by the use of appropriate cryptographic devices.

The CIIP addresses the security aspects of the initiative and needs to be endorsed by the SWG. However, initiatives cannot be executed until the MSAB issues a valid Initiative National Accreditation Endorsement Certificate (I-NAEC) and the initiative has been approved by the C-EG.

Additionally, all participating CFBLNet sites must have a current MSAB Site -National Accreditation Endorsement Certificate (S-NAEC) before they can be connected. Timely submission of all required security accreditation certifications is essential to allow the planned start of the initiative. Failure to meet this requirement could negatively impact on participation for the rest of the initiative.

5.3 Personnel security

CFBLNet users shall hold the appropriate security clearance in accordance with the initiative security classification. It is mandatory that every participant must understand and implement the general security aspects of CFBLNet before use.

ANNEX A Frequently Asked Questions (FAQ)

Q1. How is CFBLNet funded?

Every nation and organisation funds its own part. The user funds it depending upon the nation they represent. For European countries and organisations, a fee at national level is charged on an annual basis for the use of the network. Other countries cover their costs by other means. All nations provide resources for staff to attend required meetings that maybe via virtual collaboration platforms teams or physical attendance.

Q2. How is an initiative funded?

The relevant participants through national organisation service models fund initiatives.

Q3. What is an enclave?

This is a permanent or temporary closed federated network with dedicated classification and releasability in support or at least one or more initiatives. This is physically separated from other enclaves.

Q4. What do the coloured enclaves mean?

These relate to different classifications and data releasability for an initiative.

Q5. Can we have a bilateral connection?

Yes provided all criteria are met, however data maybe releasable to other nations.

Q6. If I have internet/broadband, why do I need CFBLNet, (is your information public ?)

To insure data, confidentiality integrity, availability and protection of an initiative. All data is protected with required caveats and releasability.

Q7. Who is part of the CFBLNet?

This comprises over 35 mission partners, national / organisations including defence, industry and academia (sponsored by relevant national defence organisations).

Q8. Can anyone be involved in CFBLNet?

In principle Yes if sponsored by a CFBLNet core mission partner and accepted unanimously by the CFBLNet community.

Q9. What are the benefits of CFBLNet?

A community sharing principles and practises to enable assured experimentation testing etc using established networks readily available with agreements in place.

Q10. Who are the current customers?

Depends on the requirements but can include users from experimentation and multinational capabilities dedicated to training events.

ANNEX B Glossary and abbreviations

Term	Meaning
APAN	All Partners Access Network provides tools to support the CFBLNet community.
black backbone (Blackbone)	The common CFBLNet, closed, unclassified routed IPv4/IPv6 network layer implemented using a mixture of bearer networks transporting encrypted traffic throughout the network.
C5ISR	Command Control Communications Computers Cyber Intelligence Surveillance and Reconnaissance
CCEB	Combined Communications Electronics Board, comprising Australia, Canada, United Kingdom and New Zealand.
C-EG	CFBLNet Executive Group: the oversight group of the CFBLNet, answerable to the C-SSG.
CEM	CFBLNet Engineering Meeting. Normally held in October and typically hosted in the US. Attendees at this meeting include C-EG, secretariat, LRs and WG representatives.
CFBLNet	The Combined Federated Battle Laboratories Network is a multinational, research, development, trials, assessment, exercises, testing and training infrastructure on an IP network. The term also covers the supporting staff, working groups and management structure.
CIIP	CFBLNet Initiative Information Package
CLR	Core mission partner Lead Representatives act as the central point of contact for the coordination of CFBLNet activities for their CMP.
CMM	CFBLNet Management Meeting is facilitated by the secretariat and hosted by a CFBLNet MP. It is attended by the C-EG, secretariat, LRs, WG representatives. The initiative sponsors of proposed initiatives and other persons can be invited by the C-EG or LRs as required. Normally held in April / May and is hosted on a rotational basis by members of the CCEB and NATO countries.
CMP	Core Mission Partner are member nations and belong to one of the three: USA, CCEB or NATO. Each CMP has one lead person known as the CMP Lead Representative (CLR).
Core network services	Robust, reliable and stable services which have been developed and deployed on the CFBLNet permanent components to support initiatives.
CPT	CFBLNet Productivity Tool: CPT is a Sharepoint-based tool that is used to facilitate Initiative planning and serve as a CIIP repository.
C-SSG	CFBLNet Senior Steering Group: a flag-level steering group that provides strategy on CFBLNet matters. There is one representative from each group which includes the USA, CCEB and NATO.
EEAS	EU External Action Service

Term	Meaning
Enclave	An enclave is created for a period to support the execution of one or more initiatives operating over the Backbone at a specific level of classification and releasability.
EUMS	European Union Military Staff is the directorate general of the EU External Action Service (EEAS) that contributes to the EUs common security and defence policy.
FAQ	Frequently Asked Questions
GMP	Guest Mission Partners are not CMPs but are MPs sponsored by a CMP and subject to the approval from the C-SSG.
GLR	A Guest mission partner Lead Representative is the central point of contact for the coordination of CFBLNet activities of one GMP.
IMWG	Information Management Working Group: consisting of nominated MP representatives dealing with all publications of CFBLNet in collaboration with the secretariat.
Initiative	An initiative is an activity utilizing the CFBLNet for exercises, tests, trainings, trials or experiments.
Initiative lead	The person responsible for coordinating among the participating members for the planning, execution and reporting on an initiative. The initiative lead is identified on the CIIP, coordinates with the LR and may be required to brief the initiative at any occasion.
I-NAEC	Initiative National Accreditation Endorsement Certificate
IP	Internet Protocol
ISA	Information Sharing Agreement
IWG	Initiatives Working Group assisted by the secretariat manages the CFBLNet initiative process (using CPT-CIIP).
LR	Lead Representative represents either a CMP or a GMP.
MP	Mission Partner representing either a CMPs or a GMP.
MoA	Memorandum of Agreement
MPCO	Mission Partner Capability Office
MSAB	Multinational Security Accreditation Board
NAEC	National Accreditation Endorsement Certificate: completed by the MPs accreditation authorities and sent to the MSAB board (see S-NAEC and I-NAEC).
NATO	North Atlantic Treaty Organisation
NCC	Network Control Center
NSA	National Security Agency
NTP	Network Time Protocol

Term	Meaning
NWG	The Network Working Group consisting of nominated MP SMEs deals with all network aspects of CFBLNet.
PoC	Point of Contact
PoP	Point of Presence
Secretariat	Acts as the central point for the coordination of day-to-day management of activities of the CFBLNet on behalf of the C-SSG and C-EG and assisting the LRs and WGs.
SME	Subject Matter Expert has expert knowledge in a particular area.
S-NAEC	Site National Accreditation Endorsement Certificate
Strategic Plan	A document maintained by the C-EG on behalf of the C-SSG which provides the strategic plan for CFBLNet together with rationale and action plan.
SWG	The Security Working Group consisting of nominated MP SMEs deals with all security aspects of CFBLNet.
VoIP	Voice Over Internet Protocol used for network bound telephony.
WAN	Wide Area Network
WG	Working Group