

UNCLASSIFIED

# **COMBINED FEDERATED BATTLE LABORATORIES NETWORK (CFBLNet)**



## **PUBLICATION 1 ANNEX D**

### **NETWORK OPERATIONS (Network/System Aspects of CFBLNet)**

**Version 6.0  
October 2009**

UNCLASSIFIED

## DOCUMENT CONTROL AND TRACKING METADATA

<b>Security Classification</b>	Unclassified
<b>Access Status</b>	Version 6.0
<b>Usage Condition</b>	Publicly Releasable

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

<b>Function Descriptor</b>	Network Operations (Network/Systems Aspects of CFBLNet)
<b>Activity Descriptor</b>	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, Annex D, Version 6.0

## TABLE OF CONTENTS

<b>CHAPTER 1 - INTRODUCTION.....</b>	<b>5</b>
Purpose.....	5
Authority.....	5
Amendments .....	5
Effective Date .....	5
<b>CHAPTER 2 - NETWORK OVERVIEW DESCRIPTION.....</b>	<b>6</b>
Infrastructure.....	6
CFBLNet Sites.....	7
Cryptographic Services (See also Pub 1 Annex C) .....	7
<b>CHAPTER 3 - MANAGEMENT ASPECTS .....</b>	<b>8</b>
Introduction.....	8
Management Strategy .....	8
MNIS PMO.....	8
NATO C3 Agency .....	8
Incident Management.....	8
Network Documentation.....	8
Documentation Guidelines.....	9
<b>CHAPTER 4 - NETWORK SERVICES OVERVIEW.....</b>	<b>10</b>
General.....	10
Core Network Services .....	10
Internet Protocol (IP) Address Space.....	11
<b>CHAPTER 5 - CFBLNET BLACKBONE .....</b>	<b>12</b>
General.....	12
Routing Protocols.....	12
Network Management.....	12
<b>CHAPTER 6 - BLUE ENCLAVE CORE NETWORK SERVICES .....</b>	<b>13</b>
General.....	13
Domain Name Service (DNS) .....	13
Electronic Mail (e-mail).....	13
E-mail Account Naming Convention.....	13
Web Services .....	14
Network Time Protocol (NTP) .....	14
IP Telephony.....	14

**\*APPENDIX 1 -- CFBLNET LEVEL 0 TOPOLOGY**

**\*\*APPENDIX 2 -- BLACK IP ADDRESS SPACE ALLOCATION**

**\*\*APPENDIX 3 -- CFBLNET VOIP PHONE NUMBER RANGES**

\* These Appendices are included in another document.

\*\* Unabridged version of this appendix is contained in another document.

## CHAPTER 1 - INTRODUCTION

### Purpose

101. Annex D to the CFBLNet Publication 1 contains the network operations and system management policies and procedures, related to the operations of the CFBLNet, which functions under the authority of the CFBLNet Technical Arrangement (Charter). It comprises a main body and a range of appendices. Appendices that may not be visible have been deemed to be of a sensitive nature and are available only in a classified controlled version.

### Authority

102. CFBLNet Pub 1 Annex D is issued by the CFBLNet Executive Group (C-EG) on behalf of the CFBLNet Senior Steering Group (C-SSG). The provisions of this and all associated publications shall govern the conduct of all network activities performed by the CFBLNet participants, subject to their respective Nation's laws and military regulations.

103. The Network Working Group (NWG) is the technical body, comprised of appropriate experts from the Charter Mission Partners (CMPs), which supports the network governance process for the CFBLNet on behalf of the C-EG. The terms of reference and responsibilities of the NWG are described within Annex A.

### Amendments

104. CFBLNet Pub 1 Annex D may be amended when the NWG determines that there is an identified requirement. The NWG Chair will propose the text of the amendment to the NWG members for endorsement. Once the NWG members have endorsed the amendment, it will be submitted for C-EG approval. Upon approval by the C-EG, the Secretariat will re-issue a new version of Annex D.

### Effective Date

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

## CHAPTER 2 - NETWORK OVERVIEW DESCRIPTION

### Infrastructure

201. The CFBLNet infrastructure is a closed, wide area communications network linking CMP infrastructures, collectively forming the CFBLNet. The CFBLNet Level 0 Topology is illustrated in Appendix 1 of this document. The NWG representatives are responsible for maintaining the individual CMP Level 1 and Level 2 topology diagrams with the requisite detailed information.

202. The CFBLNet consists of the following components:

- a. Black backbone (Blackbone). A common, closed, unclassified IP routed network layer implemented using a mixture of both 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 CMPs; see Chapter 5, Table D-5.1 of this document
- b. Persistent CFBL Enclaves:
  - i. CFBLNet Unclassified Enclave (CUE). A permanent IP enclave operating over the Blackbone. It will operate at the Unclassified, Non Releasable to Internet, Releasable to CMPs and to Guest Mission Partners (GMPs) level, as directed by the C-EG. The CUE will be encrypted using Advanced Encryption Standard (AES) algorithms at minimum.
  - ii. Blue Enclave. A permanent classified IP network operating over the Blackbone. It operates at the SECRET level, releasable AUSCANZUKUS + NATO.
- c. Persistent Limited-Audience Enclaves:
  - i. Four Eyes Enclave. A permanent classified IP network operating over the Blackbone at the SECRET level, releasable to AUS, CAN, UK, US only.
  - ii. NATO Red Enclave. A permanent classified IP network operating over the Blackbone at the SECRET level, releasable to NATO only.
- d. Initiative Enclaves. These are created for a finite period to support the execution of specific Initiatives and operate over the Blackbone Initiative enclaves will be stood up and shut down as required. 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 Initiative enclave will be the responsibility of the Initiative sponsor, unless otherwise agreed.
- e. Enclaves will operate Internet Protocol version 4 (IPv4), version 6 (IPv6) or a dual-stack IPv4/IPv6 configuration.

203. Operational control of all network devices must conform to the CFBLNet Pub 1 requirements. CMPs and GMPs are responsible for providing connectivity between their national sites and an agreed upon national/organizational Point Of Presence (POP) which will serve as their connection point to the CFBLNet. See paragraph 206.

204. Initiative Participants can establish connectivity via any accredited means in accordance with CFBLNet Pub 1 Annex C.

### **CFBLNet Sites**

205. CFBLNet sites are those operational participant sites accredited through the CFBLNet security process (CFBLNet Pub 1 Annex C) and approved by the C-EG-. Each NWG member will provide an up-to-date list of new/existing sites on his/her national WAN at each CMM for informational purposes. This list does not need to include individual national/organizational Initiative sites as this is the Nation's prerogative. The NWG is not part of the site approval process.

206. National/Organizational Point Of Presence. A CFBLNet national/organizational POP is a CFBLNet site that provides a point of connectivity between different national/organizational management and administrative domains. The establishment of a peering relationship between two POPs is arranged with the consent of the CMPs involved.

### **Cryptographic Services (See also Pub 1 Annex C)**

207. Cryptographic Support. The Multinational Information Sharing Program Management Office (MNIS PMO) is responsible for the coordination of cryptographic services for the permanent components of the CFBLNet from the USA sites to National POP sites. Behind the National POP of a given CMP, that CMP will be responsible for coordinating their cryptographic services and will provide this information to the NWG. Each CMP may provide their own cryptographic support for their respective information and administrative domains or arrange other support accordingly. Initiative Sponsors that require special cryptographic services are to coordinate support through their respective CLR.

208. Encryption Devices. CFBLNet enclaves are protected by appropriate and approved encryption devices and border protection systems (BPS) accredited by CMPs for the protection, as required, of information up to and including the classification level of the enclave.

209. Keying Material (Keymat). Refer to Annex C.

## **CHAPTER 3 - MANAGEMENT ASPECTS**

### **Introduction**

301. This chapter addresses the management requirements of the CFBLNet and is intended to provide a basic understanding of the network operations and the relationship between the CMPs' management cells.

### **Management Strategy**

302. Each CFBLNet CMP provides, manages, supports and is responsible for their infrastructure, which collectively forms the CFBLNet. The MNIS PMO is recognised by the CMPs as the central body responsible for coordinating the CFBLNet management policies as defined in this Annex.

303. The CFBLNet is a 24x7-accessible network. The USA Combined Communications Control Centre (CCCC), located in Arlington, Virginia, USA is staffed appropriately to support this effort. Initiative Participant manning is based on the requirements dictated by approved CFBLNet Initiatives.

### **MNIS PMO**

304. The MNIS PMO operates and maintains the CCCC and provides the CFBLNet Secretariat resources that coordinate the use of the CFBLNet for Initiatives. The MNIS PMO is responsible for all POP connections within and to the USA WAN infrastructure. The CCCC manages and monitors CFBLNet activities and makes any pertinent information available to the CMPs during normal operating hours (16x5). The CCCC will provide extended support as required for a specific initiative as defined in the Memorandum of Agreement/Service Level Agreement (MOA/SLA).

### **NATO C3 Agency**

305. The NC3A operates and maintains the European regional POP for NATO nations, NATO organizations and Guest Mission Partners (GMPs) and also provides the cryptographic bridging between NATO, CCEB and USA environments and sponsored nations and organizations, as required.

306. The NC3A also provides administrative support for NATO nations and NATO-sponsored GMPs.

### **Incident Management**

307. The CMPs are responsible to advise the Secretariat of any CFBLNet activity that is not in compliance with CFBLNet policies and practices. Incidents reported to the Secretariat will be resolved through dialogue with the CMPs involved. If the situation cannot be resolved, then recommendations will be made to the C-EG for resolution.

### **Network Documentation**

308. Each CMP will maintain their own detailed network documentation. \*

309. There are three levels of documentation that will comply with the security classification appendix within CFBLNet Pub 1 Annex C and are not intended to conflict with CMP information security/disclosure policies:

- a. Level 0. Basic CFBLNet WAN layout drawings showing major components and generic architecture at a level detailing the national Participants and the connectivity attributes between them. (Section 1: Intra-national topology; Section 2: Enclave topology; Section 3: Cryptographic topology; Section 4: Backbone architecture);
- b. Level 1. Detailed CMP/GMP layout drawings, showing major components and generic architecture within a CMP or GMP's domain (Section 1: Topology diagram; Section 2: Enclave matrix; Section 3: Cryptographic plan per site/enclave; Section 4: Backbone); and
- c. Level 2. Detailed site layout drawings, showing IP Addresses, Host Names, cards/ports, hardware/software, versions/revisions, etc. \*

\* Each nation may share details with relevant countries according to national security standards.

### **Documentation Guidelines**

310. Microsoft Visio, Excel and PowerPoint are the preferred documentation tools. Where possible, documentation should be distributed to the NWG with the capability to drill down to network information where appropriate.

## CHAPTER 4 - NETWORK SERVICES OVERVIEW

### General

401. Each CMP maintains and operates agreed levels and types of network services for the CFBLNet permanent components in order to facilitate Initiatives. These network services inter-operate with other CMPs' services to provide a collective network community. The operation of permanent network services will be coordinated by the CCCC with each CMP's designated Network Operations Centre (NOC).

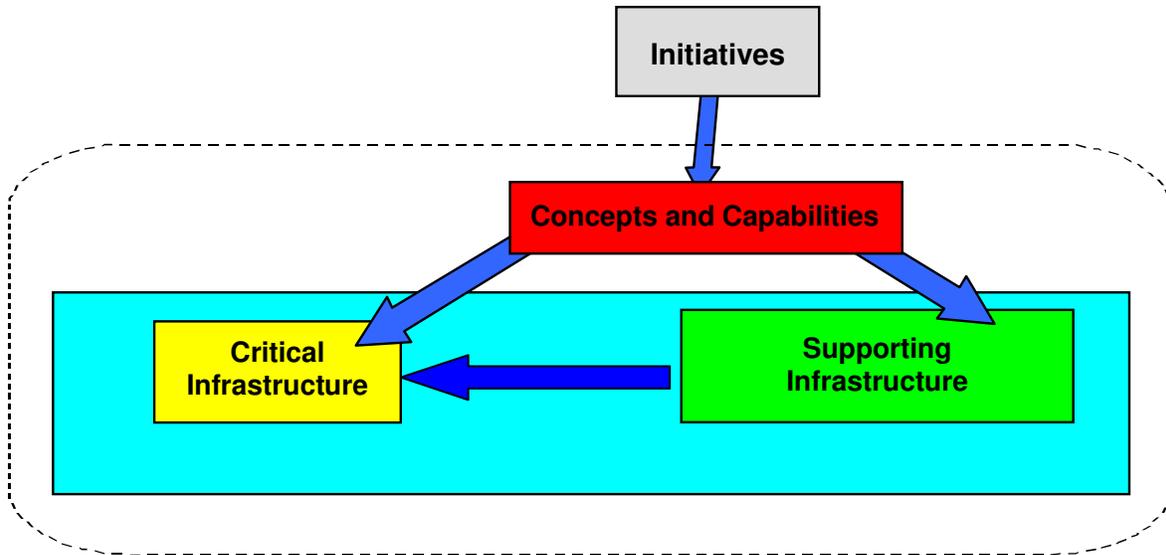
### Core Network Services

402. 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 directly by the CMPs. They are further divided into the following two categories:

- a. Critical Infrastructure. Those services that each CMP is obligated to stand up and support, as part of their minimum network infrastructure, for effective and efficient network operations; and
- b. Supporting Infrastructure. Those services that provide a value added benefit but which are not essential for effective network operations and can be hosted by any CMP on behalf of other CMPs.

403. The NWG provides recommendations to the EG on what core network services will be deployed on the CFBLNet Persistent Enclaves, its category and operational status in light of anticipated activities. It is the responsibility of the Initiative Sponsors to determine and support any network services that are required within an Initiative as these will be deemed separate from the CFBLNet Core Network Services.

404. An Initiative may deploy additional network services required to support activities specific to that Initiative. As part of the review of Initiative activities, the NWG will consider these additional network services for inclusion as part of the CFBLNet core network services for some or all of the CFBLNet permanent components. This process is managed by the NWG and follows the method illustrated in Figure D-4.1.



**Figure D-4.1, CFBLNet Network Services**

### **Internet Protocol (IP) Address Space**

405. CMPs are responsible for managing their own IP address space to support their network infrastructure requirements. IP address spaces are allocated through the NWG.

406. CMPs will use an agreed upon IP address space for the CFBLNet persistent enclaves (detailed in Appendix 2), thus minimizing the possibility of address space conflict. The CCCC is responsible for maintaining a register of all CFBLNet IP address spaces.

407. CFBLNet Initiatives, utilizing the persistent enclaves, will coordinate with their respective NWG representative to obtain IP space allocations. For those Initiatives utilizing a separate temporary enclave, NWG representatives will recommend the IP address space allocation for use within the enclave.

408. The NWG is responsible for the assignment of Border Gateway Protocol (BGP) Autonomous System (AS) numbers to each CMP.

## CHAPTER 5 - CFBLNet BLACKBONE

### General

501. The purpose of the Backbone is to provide a permanent, common, closed, unclassified transport (bearer) layer. Its primary function is to transport encrypted traffic throughout the network. There are no network services available within this component, except those required for engineering purposes, as agreed by the NWG.

502. The core network services for the Backbone are depicted in Table D-5.1.

Ser (a)	Information Service Description (b)	Status (c)
1	Internet Protocol Addressing	Required
2	Network Service Access Point Addressing	Required
3	Routing Protocols (e.g., BGP)	Required
4	Network Time Protocol (NTP)	Required
5	Internet Protocol version 6 (IPv6)	Available
6	IP Multicasting	Available
7	Bandwidth Management	Available
8	VOIP	Available

**Table D-5.1, IPv4 Backbone Core Network Services**

### Routing Protocols

503. The primary routing protocol used on the CFBLNet Backbone will be Border Gateway Protocol (BGP). Choice of routing protocol for CMP internal distribution of routes will be at the discretion of each CMP.

### Network Management

504. The CCCC will perform network management and monitoring using standard protocols (eg ICMP, SNMP). The CCCC will monitor inter-POP connectivity and the US Backbone. CMPs and GMPs may implement their own network management and monitoring tools within their own environments and uplinks. The CMPs/GMPs and CCCC will coordinate to enable visibility between environments; this may include the exchange of SNMP community strings or other details.

## CHAPTER 6 - Blue ENCLAVE CORE NETWORK SERVICES

### General

601. The Blue Enclave is a permanent classified TCP/IP routed network operating over the Backbone. It operates at the SECRET level, releasable AUSCANZUKUS + NATO.
602. The core network services for the Blue enclave are listed in Table D-6.1.

Ser (a)	Information Service Description (b)	Status (c)
1	Domain Name Service (DNS)	Required
2	E-mail (SMTP)	Required
3	Web (HTTP)	Available
4	Network Time Protocol (NTP) Source	Required
5	IP Telephony Call Manager	Required
6	VOIP phone @ each site	Required

**Table D-6.1, Blue Enclave Core Network Services**

### Domain Name Service (DNS)

603. The Blue enclave supports a distributed DNS service with each CMP being responsible for managing its own DNS domains in accordance with IETF standards.
604. The Blue enclave DNS is a federation of DNS servers, with the USA and GBR providing a dual ‘.’ root master with other CMPs and NATO assigned with a secondary ‘.’ root. Each CMP has the primary DNS responsibilities for their individual domain space.

### Electronic Mail (e-mail)

605. The Blue enclave supports a distributed e-mail service between CMPs. E-mail is considered a critical infrastructure service.
606. Simple Message Transfer Protocol (SMTP) is the agreed e-mail protocol between CMPs. CMPs may implement their own national e-mail protocols, ensuring they provide an SMTP interface at their national/organizational POP boundary.
607. In general, e-mail on the Blue enclave is routed according to the DNS Mail Exchange (MX) record. Other (e.g. static) mail routing can be implemented as agreed between CMPs.

### E-mail Account Naming Convention

608. Participant will establish e-mail accounts as either:
- a. Permanent accounts for management or engineering purposes; or
  - b. Temporary accounts for each Initiative as required.

609. There are three types of accounts that can be used in the Blue enclave to effect communications between users as listed in Table D-6.2.

<b>Ser (a)</b>	<b>Account Type (b)</b>	<b>Example (c)</b>
1	Personnel—normally used for enduring accounts (management, engineering etc)	bill.smith@, felicity.smith@
2	Organizational—normally used for operational/warfighter accounts	cflcc.g6@, <a href="#">asbde.s3@uk3cdobde.s2</a>
3	Group—for address lists	CCCC.staff@, cflcc.staff@

**Table D-6.2, Blue Enclave E-mail Account Strategy**

610. The recommended convention for Blue enclave e-mail accounts is:  
**<first name>.<last name>**

### Web Services

611. The Blue enclave supports the Web service (HTTP and HTTPS) protocols to provide Web services across the Blue enclave for management and engineering coordination as well as the delivery of Web-based information sources and products for initiatives.

612. CMPs are actively encouraged to populate these Web services in support of information dissemination for the purposes of CFBLNet management/coordination and to support Initiatives. CMPs should advise the NWG when a permanent or temporary Website is established in the Blue enclave.

613. Should classified CFBL information need to be made available, a website will be stood up in the Blue enclave.

### Network Time Protocol (NTP)

614. The Blue enclave supports the Network Time Protocol (NTP) in order to provide a stable time source, synchronized across the wide area.

615. A Stratum 1 time source located at the NATO PoP is the primary NTP source for the Blue enclave. AUS, CAN, NZL, GBR, NATO and the MNIS PMO routers are peered with each other. Other CMPs will establish a one way server relationship with their nearest time source.

### IP Telephony

616. The Blue enclave supports IP Telephony (VoIP) for inband secure communications between the CMPs. It is also the primary means of secure communications for the CFBLNet management and engineering communities.

617. Each Blue enclave site should have at least one VoIP (hardware or software phone) capability onsite as a minimum that is compatible with the Blue enclave standard system. This phone is primarily for engineering management and coordination. Each site must coordinate with a “Call Manager-enabled” site to have its VoIP phone managed.

618. The Voice over IP (VoIP) Phone Numbers allocated for the Blue enclave are detailed in Appendix 3.

APPENDIX 1 -- CFBLNET LEVEL 0 TOPOLOGY

