

UNCLASSIFIED

COMBINED FEDERATED BATTLE LABORATORY NETWORK CFBLNet



Basic Guide to CFBLNet Accreditation Procedures

**Version 2.00
October 2009**

UNCLASSIFIED

TABLE OF CONTENTS

BASIC GUIDE TO THE CFBLNET ACCREDITATION PROCEDURES	2
Purpose of the Document.....	2
Accreditation Requirements.....	2
Overview.....	2
Accreditation Certificates	2
Security Accreditation Authorities	3
National/Organizational Accreditation Authorities	3
Multinational Security Accreditation Board (MSAB).....	3
ACCREDITATION PROCEDURES	4
Site Accreditation.....	4
Initiative Accreditation	4
FREQUENTLY ASKED QUESTIONS – FAQ	5
Initiation.....	5
Site Accreditation.....	5
Systems Accreditation	6
CIIP Process.....	6
Testing.....	7
Execution	7

BASIC GUIDE TO THE CFBLNET ACCREDITATION PROCEDURES

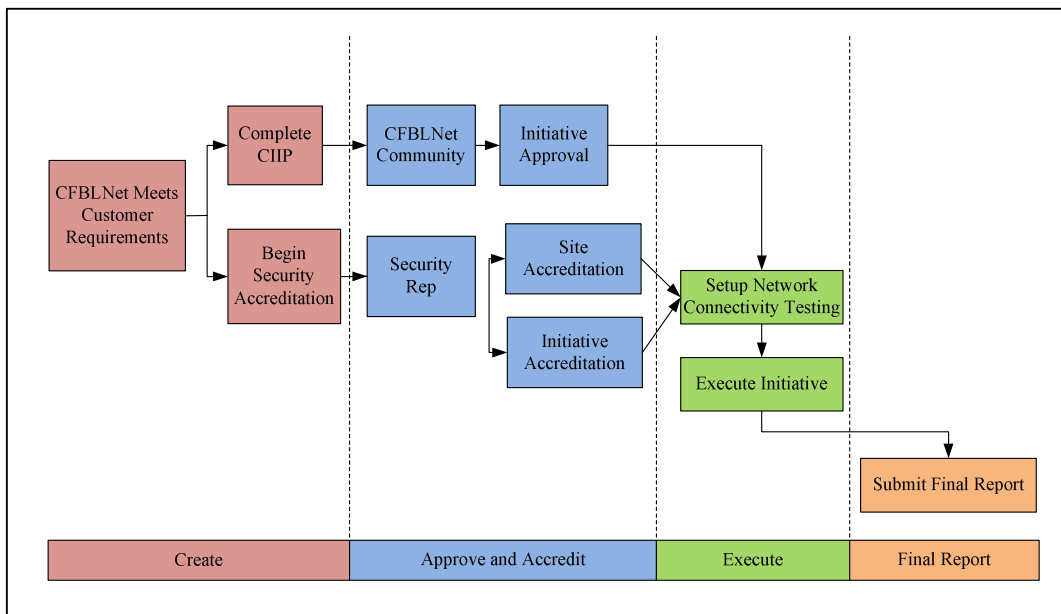
Purpose of the Document

The purpose of this document is to provide an overview of the CFBLNet accreditation requirements and procedures as well as the roles and responsibilities of the authorities involved in the accreditation process.

Accreditation Requirements

Overview

The accreditation process can be seen as a process parallel but independent of the CFBLNet Initiative Information Pack (CIIP) approval process (which is fully described in Annex B of Publication 1).



Sites must be accredited before they can pass data and be considered official CFBLNet Site(s). An Initiative Accreditation certificate must be obtained for a given site in order to use the CIS at this site.

Accreditation Certificates

A Site-National Accreditation Endorsement Certificate (S-NAEC) 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 National/Organizational Accreditation Authority.

An Initiative-National Accreditation Endorsement Certificate (I-NAEC), 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.

Security Accreditation Authorities

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

National/Organizational Accreditation Authorities

National/Organisational Accreditation Authorities are responsible for the accreditation of all infrastructure and services located behind their defined national/organisational boundary and/or Point of Presence (POP).

National/Organisational Accreditation Authorities are also responsible for ensuring that each proposed Site and/or Initiative under their responsibility has met similar standards for accreditation.

Accreditations packages are first issued by the appropriate National/Organisational Accreditation Authorities, who submits the request and accreditation information to their national/organisational MSAB representative for an endorsement certificate.

Multinational Security Accreditation Board (MSAB)

The MSAB is the security accreditation endorsement authority for activities executing on systems crossing national or organisational boundaries including CFBLNet.

When all national/organisational 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 an information copy to the U.S. MultiNational Information Sharing (MNIS) Program Management Office (PMO).

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

ACCREDITATION PROCEDURES

Site Accreditation

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

When the Site/Local Accreditation Authority has determined that the site has met the specified security requirements, he sends the Site Accreditation package to the National/Organisational Accreditation Authority for approval.

When the National/Organisational Accreditation Authority has determined that the Site has been accredited in accordance with (IAW) national/organisational and CFBLNet standards he submits the accreditation package to the MSAB Representative for Endorsement. The MSAB Representative then determines whether the Site has been accredited in a manner which satisfies national/organisational and CFBLNet requirements.

When the national/organisational MSAB Representative has endorsed the site accreditation they completes the S-NAEC and notify the MSAB Chair and MSAB members that the site has an approval to operate and send an informational copy to the Security Coordinator of the U.S. MNIS PMO.

Initiative Accreditation

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

When the National/Organisational Accreditation Authority has determined that the Initiative correctly implements the national/organisational security standards he submits the accreditation package to the national/organisational MSAB Representative for Endorsement. The MSAB Representative then determines whether the Initiative has been accredited in a manner which satisfies national/organisational policies including CFBLNet requirements.

When the national/organisational MSAB Representative has endorsed the site accreditation they complete the S-NAEC and notify the MSAB Chair and the MSAB members that the site has approval to operate and send an informational copy to the Security Coordinator of the U.S. MNIS PMO.

FREQUENTLY ASKED QUESTIONS – FAQ

Initiation

Question	Answer
<i>Do I need accreditation for UNCLASSIFIED Initiatives?</i>	<i>Yes, since you will be exchanging data with coalition partners.</i>
<i>When should I start the security paperwork?</i>	<i>As soon as you can. It can take from one to four months to get your Initiative accredited.</i>
<i>Where do I send the security paperwork?</i>	<i>To your National Accreditation Authority (or NATO Office of Security for NATO). Your National/Organizational lead can help you. In turn it will be forwarded to MSAB for endorsement.</i>
<i>Who agrees all sites to be connected for an Initiative?</i>	<i>Initiative lead shall agree all sites to be connected.</i>
<i>Can Non Chartered Nations or Guest Mission Partners (GMP) participate?</i>	<i>If the Initiative involves a non CFBLNet chartered Nation or GMP then that Nation or Organisation must obtain sponsorship from a chartered Core Mission Partner (CMP). That Nation or Organisation would then be responsible for ensuring that the connecting system is accredited to their Nation or Organisation security standards. The detailed procedure can be found in Pub 1 Annex C.</i>

Site Accreditation

Question	Answer
<i>How can I know if a given site is accredited or not?</i>	<i>Your MSAB Rep will provide you the list of all accredited national sites.</i>
<i>What if a site I'm considering is not on this list?</i>	<ul style="list-style-type: none"> <i>- If a site accreditation has expired it should be reaccredited.</i> <i>- New sites should be nominated by the CFBLNet Lead Representative and follow appropriate accreditation procedures.</i> <i>- The initiation of this procedure will allow the inclusion of this site within the CIIP proposal.</i>

Systems Accreditation

Question	Answer
<i>What information do I need to gather regarding the system(s) to be connected?</i>	<ul style="list-style-type: none"> - As a minimum, you need to know to which level your system(s) has been accredited. - This information will be provided to you by your National Accreditors. - In case of doubt, your CLR will confirm who is your National Accrerator.
<i>What if my system(s) to be connected are not already accredited?</i>	<i>Then you should obtain the accreditation templates from your National Accrerator and start the local accreditation process.</i>
<i>What are the security regulations for networking across the CFBLNet?</i>	<i>All security rules and regulations are laid down in Pub 1 Annex C.</i>

CIIP Process

Question	Answer
<i>What is the purpose of the CIIP?</i>	<i>Systems may be connected together through the CFBLNet with the CFBLNet Management permission. This permission can only be obtained by the completion and approval of the CIIP.</i>
<i>When does the CIIP need to be submitted?</i>	<ul style="list-style-type: none"> - Only when all systems are accredited or are in the process of being accredited can this CIIP process be started. - Please note that the CIIP and Accreditation processes support two different objectives and, as a consequence, can be run in parallel.
<i>Who fills the CIIP template?</i>	<i>The lead of the Initiative will fill up this template.</i>
<i>What is needed from me?</i>	<i>You should provide the Initiative lead all the information that will allow him to complete all the sections of the CIIP. In particular, a complete network diagram will have to be provided.</i>
<i>Who officially submits the CIIP?</i>	<i>The CLR of the Initiative Lead will submit the CIIP to the CFBLNet Community.</i>
<i>How much time does it take to get the CIIP approved?</i>	<i>Review and Approval of the CIIP by the CFBLNet community will take between 30 (for simple Initiative) and 45 days (for larger Initiatives)</i>

Testing

Question	Answer
<i>When can I start initiative testing over the CFBLNet Network?</i>	<i>As soon as the CIIP is approved and, provided that 1) two or more sites within the same Initiative have been approved and 2) the Initiative itself has been approved by the MSAB for testing (ATT).</i>
<i>Which document do I need to start this testing?</i>	<i>A valid site S-NAEC and an initiative I-NAEC or an approved ATT issued by the MSAB Rep.</i>
<i>What are the limits of this testing?</i>	<i>The limits of testing will be defined in the accreditation documentation issued by the MSAB.</i>

Execution

Question	Answer
<i>When can I start executing the Initiative over the CFBLNet Network?</i>	<i>Execution can start as soon as the CIIP is approved by the CFBLNet Community and the Sites and Initiative are endorsed by the MSAB.</i>
<i>What if all the Sites are not approved yet?</i>	<i>- If all the Sites are not approved yet, then the MSAB Rep can authorise partial execution of approved sites. - Unauthorised sites will not be able to participate in an Initiative.</i>
<i>What happens if an S-NAEC expires during the conduct of an Initiative?</i>	<i>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.</i>
<i>Who holds all this documentation?</i>	<i>The MSAB Chair, MSAB Groove Workspace, and the Security Coordinator of the U.S. MNIS PMO.</i>