

**DIGITAL INTEGRATION LABORATORY
(DIL)**



**CONFIGURATION MANAGEMENT PLAN
(CMP)**

18 May 2012

Table of Contents

1.0	INTRODUCTION.....	1
1.1	REFERENCES	1
1.2	PURPOSE.....	1
1.3	BACKGROUND	1
1.4	SCOPE.....	2
1.5	DOCUMENT OVERVIEW.....	2
2.0	NETWORK OVERVIEW.....	2
2.1	FIGURE 2.1 DIL DATA FLOW AND NETWORK ARCHITECTURE BOUNDARY.....	3
3.0	ORGANIZATIONS AND RESPONSIBILITIES.....	4
3.1	PEO STRI	4
3.2	ARMY PROGRAM MANAGERS	4
3.3	CTSF CONFUIRATION MANANGEMENT OFFICE (CMO)	4
3.4	DIL PERSONNEL.....	4
4.0	DN CM ENTITIES.....	4
4.1	DN WORKING GROUP.....	4
5.0	CONFIGURATION MANAGEMENT ACTIVITIES.....	4
5.1	ESTABLISHMENT OF DN PLANNING DOCUMENTATION.....	5
5.2	DIL NETWORK ARCHITECTURE BOUNDARY CONFIGURATION CONTROL BOARD	5
5.2.1	PEO STRI DIL CCB MEMBERSHIP	5
	TABLE 1 DIL CCB MEMBERSHIP ROLES	6
5.2.2	PEO STRI DIL CCB RESPONSIBILITIES	6
5.3	CHANGE MANAGEMENT FOR AIC SUPPORT.....	6
6.0	PEO STRI DIL SOFTWARE BLOCKING (SWB) SUPPORT.....	7
7.0	FEDERATED NET-CENTRIC SITES	7
8.0	CTSF CMO SOFTWARE SUPPORT PROCESS.....	8
8.1	MATERIAL FIELDING EXCEPTION (MFE).....	8
8.2	IAVM AND SECURITY PRODUCTS.....	8
9.0	DIL SIM/STIM, INSTRUMENTATION & DATA COLLECTION TOOLSETS.....	8
10.0	CTSF CONFIGURATION MANAGEMENT WEBSITE.....	9

1.0 INTRODUCTION

The PEO STRI Digital Integration Laboratory (DIL) was established in 2001 the intent of which is to gain efficiencies in how PEO STRI programs interfaced with Army Mission Command (MC) Systems. The DIL is provides resources and services necessary to sustain a centrally controlled risk reduction and integration facility supporting the integration of the Army's System and Non-System Training Aides, Devices, Simulation and Stimulator with existing and emerging MC Systems and Command, Control, Communication, Computers, Intelligence, and Reconnaissance (C4ISR) Systems. The DIL supports PEO STRI program development efforts while reducing risks associated with successful completion of formal Army Interoperability Certification (AIC) testing. As such the DIL is formally recognized as an extension of the Central Technical Support Facility (CTSF) at Fort Hood, Texas, working in full cooperation with the CTSF to establish, sustain and operate representative C4ISR networks to support PEO STRI program development initiatives and to conduct formal distributed AIC via the Defense Research Engineering Network (DREN).

1.1 References

- MIL-HDBK-61A(SE), 7 Feb 2001
- PEO STRI Standard Operating Procedures(SOP) NO.25-2-5, 24 Sep. 2008
- CTSF CMO Standard Operating Procedures (SOP) V0.17, 22 Jan 2009
- CTSF CMO Configuration Management Plan (CMP) V0.05, 9 Oct 2008

1.2 Purpose

The purpose of this document is to identify and describe configuration management (CM) processes, policies, and procedures implemented for the conduct of DIL Network (DN) Operations and to ensure that the network changes occur within an identifiable and controlled environment.

30 November 2005, the CIO G/6 and the CTSF Configuration Management Office (CMO) was assigned the mission of the Army Configuration Management Office (ACMO). Accordingly, the DIL will follow and otherwise implement those CTSF processes, policies and procedures as they apply to the conduct of formal distributed AIC and other activities associated with the management and operation of the PEO STRI DIL as a designated Federated Net-Centric Site (FaNS).

This document is intended to be a living document. As the Government implements the components of this plan, and to facilitate the every changing state-of-the-art, the DIL CM processes may need to be refined. Consequently, the final version of this document should itself be placed under configuration management and the respective changes managed accordingly.

1.3 Background

The Central Technical Support Facility (CTSF) at Fort Hood, Texas is the Army's execution agent for AIC testing and certification. The CTSF has formally recognized the PEO STRI DIL as

an extension of their activity and has endorsed the PEO STRI DIL to conduct distributed AIC. Under the operational control of the CTSF, two formal distributed AIC events have been successfully conducted from the DIL.

The DIL was designated a Federated Net-Centric Site (FaNS) by the Army CIO G/6 on 05 June 2009.

1.4 Scope

The scope of this document is the identification of a top-level configuration management plan for the DIL. This plan presents CM activities for the hardware portion of DN (e.g., switches, routers, and hubs). Section 2 describes the DIL Network scope in greater detail.

1.5 Document Overview

This document is divided into the following ten (10) major sections, Introduction, Network Overview, Organization and Responsibilities, Configuration Management Entities, CM Activities, Software Blocking (SWB) Support, Federated Net-Centric Sites (FaNS), SIM/STIM, Instrumentation & Data Collection Toolsets, and CTSF CM Website,. The organization of this document is as follows:

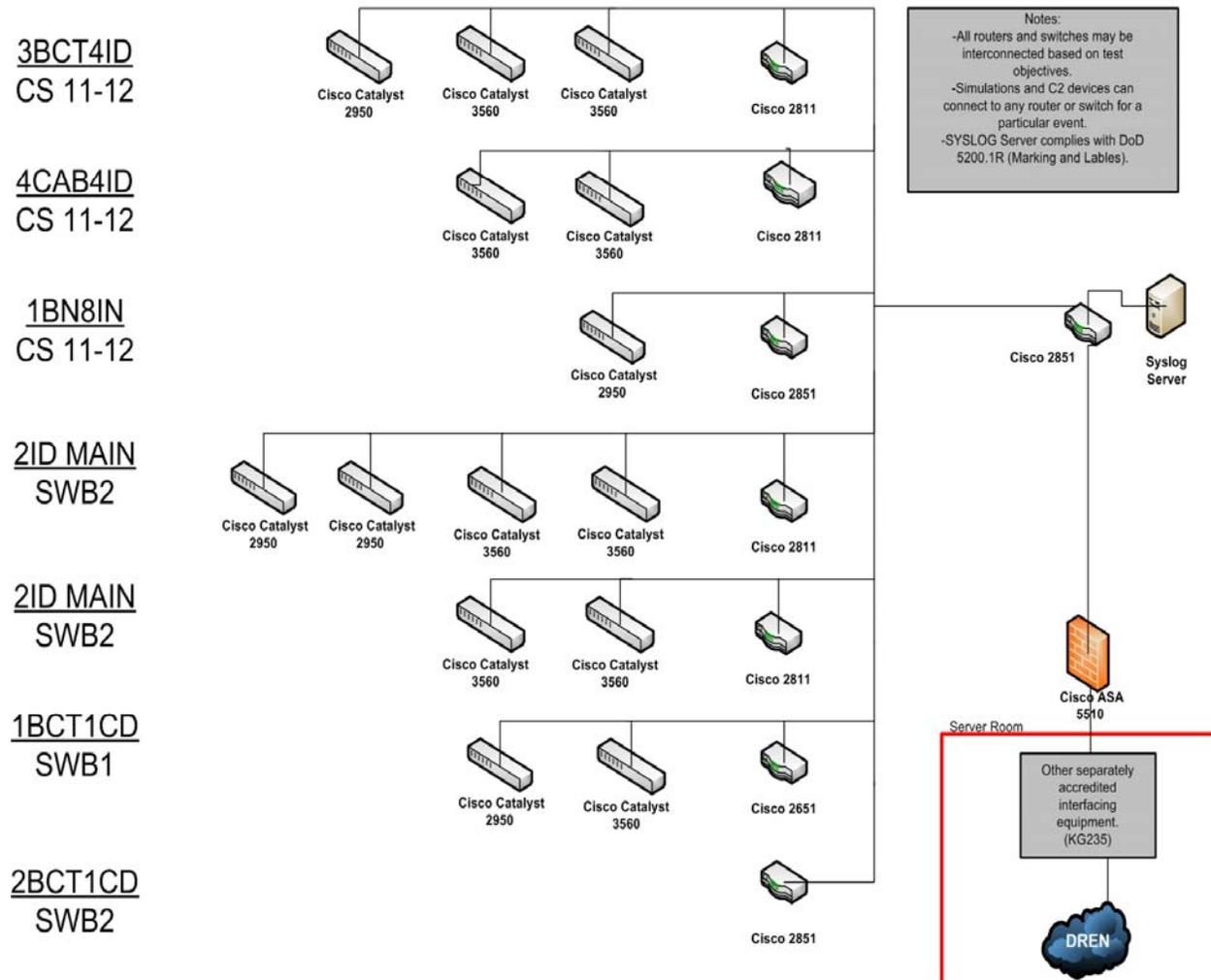
- **Section 1.0 – Introduction:** This section presents preliminary information concerning this document. The introduction provides background information about the DN. The scope of this document, the organization of this document, and any references utilized in the assembly of this document.
- **Section 2.0 – Network Overview:** This section presents an overview of the DN architecture.
- **Section 3.0 – Organizations and Responsibilities:** Establishes areas of responsibility.
- **Section 4.0 – DN CM Entities:** Defines organization CM authority and responsibility.
- **Section 5.0 – CM Activities:** Defines configuration items, documentation, and change management.
- **Section 6.0 – SWB Support:** Defines SWB support functions.
- **Section 7.0 – FaNS:** Acknowledges DIL FaNS designation.
- **Section 8.0 – CTSF CMO SW Support :** Defines CTSF CMO SW support.
- **Section 9.0 - Instrumentation & Data Collection:** Defines required toolsets.
- **Section 10.0 – CTSF CM Website:** Defines DIL access to CTSF CM Website.

2.0 DIL NETWORK OVERVIEW

The DIL Network provides connectivity for supporting DIL integration and test events. The DIL Network architecture is a modular configuration consisting of routers, switches, and instrumentation assets configured to support integration and the conduct of formal distributed test and certification. CISCO routers are configured with a switch module that facilitates direct connectivity. Separate CISCO switch platforms are used as overflow when the capacity of the switch modules has been reached. Each router is able to be "trunked" to create a LAN based representation of a specified network architecture. A separate and distinct CISCO router is used to connect to the DREN for distributed integration and test. This enables integration and

checkout of the DREN circuit without the disruption of the remainder of the DIL Network. It also provides an isolated physical control point for the DREN interface into the DIL.

DIL DATA FLOW AND NETWORK ARCHITECTURE BOUNDARY



3.0 ORGANIZATIONS AND RESPONSIBILITIES

The Program Executive Office, Simulation, Training and Instrumentation (PEO STRI) DIL and the CTSF, support distributed AIC testing via the Defense Research and Engineering Network (DREN) for all Software Blocking programs. The DIL is a component augmenting the mission of the CTSF in supporting the integration of Army Modeling and Simulation (M&S) with Army Command and Control.

3.1 PEO STRI is responsible for providing configuration management oversight for all PEO STRI simulation and stimulation training devices.

3.2 Army Program Managers who develop, field and update the Army's Mission Command System software resident in the DIL, will maintain Configuration Control of their respective products. Each software application has its own Authority to Operate. All systems are configured and operated in accordance with the Security Classification guide.

3.3 The CTSF Configuration Management Office (CMO) operates as a staff office under the CTSF and reports directly to the CTSF Director and CTSF Technical Director through designated Configuration Manager. The CTSF CMO is established as the reliable source for CM information and guidance for distributed Army Interoperability Certification testing locations and viable Federated net-Centric Sites (FaNS). The CTSF CMO provides the DN MC system software and associated data products that parallels the product versions undergoing test and integration on the CTSF test floor. PEO STRI will maintain control and accountability of the above mentioned system software and as such is not authorized to release it to other parties. All other data implemented in the DIL will be received from verifiable or trusted data sources. All COTS software used on IS systems that comprise the DIL Network Architecture boundary will be fully licensed IAW U.S. Copyright Laws.

3.4 DIL personnel are responsible for the day-to-day operation of the DN. They are responsible for maintaining the components of the DN and ensuring that the DN is maintained IAW the prevailing system and network architecture.

4.0 DN CM ENTITIES

PEO STRI, Army PMs and the CTSF will provide cross-organizational CM control and coordination.

4.1 DN Working Group

The DN WG, made up of representatives from PEO STRI and the CTSF, is a less formal change control organization that coordinates minor DN changes (e.g., changing settings on a particular router) between the entities. This DN WG provides a more streamlined CM control mechanism.

5.0 CONFIGURATION MANAGEMENT ACTIVITIES

The following activities are to be performed to guarantee consistency and standardization across the DN Architecture, while enabling configuration control of the overall DN infrastructure by monitoring, maintaining, and verifying information on all DIL CIs.

5.1 Establishment of DN Planning Documentation

DIL planning documentation will include a Configuration Item Identification List, applicable Software Baseline Version Chart, and the Army C4ISR & Standardization Initialization System (ACSIS) Data Products as distributed by the CTSF CMO. The CTSF Configuration Management Quality Assurance (CMQAv2) and Configuration Management Audit Manager (CMTSv3) databases will serve as the authoritative sources for ensuring strict identification, implementation, maintenance and reporting as required.

5.1.1 DIL SYLOG Data Back-up Procedures

DIL data backup will be performed weekly by the DIL network administrator using the following procedure:

- a. Log onto the SYSLOG Server
- b. Open the Terminal Window
- c. Copy and save log files to the designated SYSLOG backup Hard Drive

5.2 DIL Network Architecture Boundary Configuration Control Board (CCB)

The DIL CCB is the official body empowered to act upon all proposed Change Requests (CR) for the DIL network architecture boundary configuration items. The CCB provides for proper CR evaluation, processing, approval/disapproval, and implementation throughout the life cycle of the DIL. The DIL CCB meets at on a quarterly basis or as otherwise required, as determined by the DIL PD who also serves as the DIL CCB Chairperson. The DIL CCB is conducted via email or by using a standardized meeting agenda, when deemed appropriate by the CCB Chairperson. Example of a standardized meeting agenda is:

- a. Review action items of prior meeting.
- b. Review, approve, disapprove, or authorize point of contact (POC) to determine effort, cost, schedule impact, and / or re-planning for the specific CHANGE REQUEST.
- c. Special topics discussion.

The minutes of the CCB are the official vehicle for recording matters related to the DIL. The CR process is applied to assure that changes are tracked and maintained to ensure configuration management and control.

5.2.1 PEO STRI DIL CCB Membership

Membership of the CCB is identified by the Configuration Control Board Establishment Memorandum, which is published by the DIL PD (CCB Chairperson). The CCB Chairperson, will make final decisions regarding CR actions brought before the board. The Chairperson appoints CCB Secretary who is responsible for coordinating CCB meetings, prepares and publishes the agenda, records minutes of the meeting, and monitors DIL CCB action items as assigned by the Chairperson. Other members of the CCB provide recommendations to the Chairperson, but at no time can they negate final Chairperson decisions. The following individuals are appointed as members of the DIL CCB.

Table 1 DIL CCB Membership Roles

Contractor	CCB Membership/Role	Government
	Chairperson / Final Approval Authority	DIL PD
	Member / Information Assurance (IA)	DIL IAM
DIL Manager	CCB Secretariat / - Send Change Requests - Review Proposed Change Requests - Prepare Meeting Minutes	
DIL Lead System Engineer (Technical Lead)	Member/ Prepare Change Requests and submit to Secretariat for distribution	

The chairperson may request DIL CCB attendance of other personnel from other functional areas, whenever an agenda item requires further explanation or coordination.

5.2.2 PEO STRI DIL CCB Responsibilities

The DIL CCB is responsible for reviewing and assessing proposed changes to DIL Network Architecture Boundary. The DIL PD has the overall responsibility as the CCB Chairperson. DIL CCB members recommend changes for CCB consideration, and are responsible for providing technical, operational, and IA impacts of CR’s being considered. Upon receipt of final approval from the CCB chairperson, the CCB Secretariat is responsible for documentation (prepare CCB minutes) and implementation, thereby ensuring effective physical control of the DIL network architecture boundary.

5.3 Change Management for AIC Support

Change management will be accomplished in accordance with direction and guidance received from the CTSF CMO as it applies to the implementation of changes to the DN Software Baseline, and associated ACSIS Data Products. During the conduct of AIC and other formal testing, the designated CTSF Test Officer will coordinate with the CTSF CMO and provide direction for the implementation of any change(s) to the “Locked-Down” test architecture. Changes to DIL information systems and network architecture is managed and approved by the DIL manager who will ensure that all implemented data changes are backed up stored and maintained in DIL data files.

6.0 PEO STRI DIL SOFTWARE BLOCKING (SWB) SUPPORT

The PEO STRI DIL works closely with the CTSF CMO and the CTSF Test Directorate (TD) for the purpose of conducting and otherwise supporting SWB Army Interoperability Certification (AIC). For this purpose the DIL is recognized as an extension of the CTSF and as such has aligned DIL processes, policies, and procedures to ensure compliance with the same. PEO STRI DIL supports Army Capability Sets Insertion transforming from current baseline strategies to more effectively integrate and synchronize delivery of PEO STRI Training Simulation and Stimulation Training Devices to the Warfighter.

In compliance with the stipulation of the Army Interoperability Certification Policy, the CTSF shall be responsible for conducting Block certification. HDQA CIO/G-6 maintains the ownership and responsibility for the AIC Baseline. CTSF CMO will provide and verify the DN architecture and AIC Baseline to ensure compliance.

CTSF policy for formal interoperability testing focuses on end-to-end, multi-thread/multi-echelon testing with realistic operational simulation and stimulation based on information and data exchanges. For this purpose the CTSF will assign an Operations Coordinator and Test & Evaluation Test Officer to perform all required coordination of these events.

During the conduct of formal AIC the portion of the DN that is designated as part of the formal certification and test architecture will be under the operational control of the designated CTSF Test Officer for the duration of the formal test and certification event. Accordingly, changes to the architecture under test will not be implemented without prior coordination and approval of the designated CTSF Test & Evaluation Management “Pit Boss”. In support of these events the PEO STRI DIL will provide an isolated environment on a physically secure architecture with tight CM procedures and Information Assurance Compliance.

PEO STRI Systems undergoing AIC testing will be placed under CTSF CM control throughout the execution of the certification and test event. Physical configuration auditing (PCA) will be conducted by the CTSF CMO and/or security scanned by CTSF Information Assurance or other designated DIL personnel to ensure network compliance. It remains the responsibility of the respective PEO STRI Material Developer (MATDEV) to coordinate directly with the responsible CTSF Test Officer and to be cognizant of and to ensure compliance with all AIC Entrance and Exit Criteria.

7.0 FEDERATED NET-CENTRIC SITES

The Federated Net-Centric Sites (FaNS) are a federation of existing Army and Joint (when applicable) facilities, network-connected together to execute horizontal and vertical integration and Army Interoperability Certification (AIC) testing and Configuration Management for applicable Army Information Technology/National Security Systems (IT/NSS) across all MA/Domains. The FaNS Environment supports the expansion of HQDA CIO/G-6’s mission of validating interoperability and Net-Centricity of all Army IT/NSS. The FaNS Environment and its methodologies will provide the Army with an agile, efficient, flexible and persistent distributed integration and interoperability testing capability.

Deputy Chief of Staff Army, Chief Information Office (CIO/G-6) has designated and accredited the CTSF as the Federated Net-Centric Site **Nucleus** and being the Warfighter Mission Area (WMA) Army Interoperability Certification (AIC) Test Agent.

CTSF's Configuration Management Office as the Army Configuration Management Office (ACMO), and as such ICW CTSF's Test & Evaluation Management Test Operations and CECOM-LCMC FaNS will provide guidance, assistance and support PEO STRI DIL related FaNS integration and test support activities.

HQDA CIO/G-6 Accreditation Cell supports the FaNS by conducting AIC Site Accreditation and Inspections prior to final FaNS designation. Accordingly, the PEO STRI DIL will successfully undergo the FaNS accreditation process to ensure compliance as a precondition for receipt of the HQDA CIO/G-6 FaNS Accreditation Letter.

8.0 CTSF CMO SOFTWARE SUPPORT PROCESS

CTSF CMO supports the acquisition, management, distribution and accountability of certified Mission Command (MC) software for the PEO STRI DIL and designated FaNS by enforcing compliance with the strict guidelines and practices that were implemented to ensure configuration control of all associated configuration items.

8.1 Material Fielding Exception (MFE)

CTSF CMO in support of CECOM/LCMC Material Fielding Exceptions to rapidly develop, field, and support leading edge, survivable, secure and interoperable tactical, theater and strategic command, control and communications systems, will issue and ship approved Army Interoperable Fielded Baseline configuration items and their updates IAW signed Memorandum of Agreement. CTSF CMO license agreement practices will be enforced.

8.2 IAVM and Security Products

Each quarter, the Information Assurance Vulnerability Management (IAVM) Disc is received by the CTSF CM through the CTSF Information Assurance Team. The CTSF CMO will ship the IAVM Disc to the PEO STRI DIL and other current Materiel Exception Fielding customers. The PEO STRI DIL will implement the IAVM updates as required quarterly or as otherwise directed by the designated CTSF Test Officer during the conduct of formal AIC events.

9.0 PEO STRI DIL SIM/STIM, INSTRUMENTATION & DATA COLLECTION TOOLSETS

During AIC and other test events, networks are monitored to support CTSF analysis in an effort to enhance WARFIGHTER network performance. All tools used during the conduct of CTSF supported test events will mirror those tools used on the CTSF test floor.

10.0 CTSF CONFIGURATION MANAGEMENT WEBSITE

The PEO STRI DIL has been granted permission to utilize the CTSF Configuration Management website. The DIL uses this website as its authoritative source for the use of all supported baselines and data products. This repository of information provides requisite information needed to assist the DIL with managing and maintaining up to date product and services information for DIL operations. The Configuration Managements website contains current baselines for SWB I, SWB II or the next generation of SWB testing as well as baselines which are currently under test.