

UNCLASSIFIED



**Net-Enabled Command Capability
INCREMENT 1
INFORMATION ASSURANCE VULNERABILITY
MANAGEMENT (IAVM) PLAN**

Version 1.0

28 May 2008

CM # INC1-IAVM-00035

Prepared by:

Net-Enabled Command Capability
Joint Program Management Office (JPMO)
P.O. Box 4502
Arlington, VA 22204-4502

In Collaboration with the US Joint Forces Command and NECC Component Program Manager's
for Navy, Air Force, Army, Marine Corps and DISA.

DISTRIBUTION – Distribution authorized to DoD and DoD Contractors only; for administrative/operational use
(May 2008). Other requests for this document shall be referred to the NECC Program Management Office.

DESTRUCTION NOTICE – For unclassified, limited documents, destroy by any method that will prevent
disclosure of contents or reconstruction of the document.

UNCLASSIFIED

This document contains information exempt from mandatory disclosure under the Freedom Of Information Act (FOIA).
Exemption 2 applies.

UNCLASSIFIED

APPROVAL PAGE

Approved by: Laura D. Knight

Date: 5/28/08

LAURA D. KNIGHT

Program Manager,
Joint Program Management Office (JPMO),
Net-Enabled Command Capability (NECC)

UNCLASSIFIED

UNCLASSIFIED

EXECUTIVE SUMMARY

The Net-Enabled Command Capability (NECC) is the Department of Defense's (DoD's) principal program for Command and Control Capabilities (C2C) that will be accessible in a net-centric environment and will focus on providing the commander with the data and information needed to make timely, effective, and informed decisions. The NECC Information Assurance Vulnerability Management (IAVM) Plan presents a streamlined approach for responding to IAVM notifications published by the Joint Task Force-Global Network Operations (JTF-GNO). This approach is designed to meet the DoD's requirement to address vulnerabilities as well as NECC's requirement to maintain configuration management of Capability Modules (CMs). In the NECC's IAVM, Component Program Management Offices (CPMOs) monitor IAVM notifications and test the operational impact of IAVM fixes while coordinating with the Configuration Control Board (CCB). Also, the Vulnerability Management System (VMS) will be used to track the status of IAVM notification compliance at Defense Information Systems Agency (DISA) installations.

UNCLASSIFIED

UNCLASSIFIED

REVISION HISTORY

REVISION NUMBER	REVIEWER / ORG	CHANGES	REVISION DATE	DATE ENTERED	NAME OF PERSON ENTERING CHANGE
0.0.2	E. S. Koehler/ NECC	Accepted Dustan Brown edits. Made changes to IAVM process based on consultation with knowledgeable source. Reduced the number of signers on Approval page.	25 November 2007	25 November 2007	E. S. Koehler
0.0.3	E. S. Koehler/ NECC	Updated based on adjudicated comments.	13 December 2007	13 December 2007	E. S. Koehler
0.0.4	E. S. Koehler/ NECC	Updated based on adjudicated comments.	30 January 2008	30 January 2008	E. S. Koehler
0.0.4	DLB/JPMO	Edited document, corrected references, inserted footnotes that reference documents, hyperlinked reference documents, formatted (graphics, table, figure, TOC, TOF, TOT), fixed Headers and Footers, and corrected acronyms.	8 Feb 2008	8 Feb 2008	Dustan Brown
0.0.5	E. S. Koehler/ NECC	Updated based on late comments and input from 1 May IA WIPT.	19 May 2008	19 May 2008	E. S. Koehler
0.0.6	DLB/JPMO	Reviewed author's input/changes. Minor edits and formatting.	20 May 2008	20 May 2008	Dustan Brown
1.0	DLB/JPMO	Final formatting and corrected all acronyms	28 May 2008	28 May 2008	Dustan Brown

TABLE OF CONTENTS

APPROVAL PAGE.....II

EXECUTIVE SUMMARY III

REVISION HISTORY IV

1 INTRODUCTION.....1

1.1 OBJECTIVE 1

1.2 SCOPE..... 1

1.3 REFERENCE DOCUMENTS 2

2 DISA IAVM PROCESS BACKGROUND.....2

2.1 DoD VULNERABILITY NOTICES 2

2.2 NECC IAVM IMPLEMENTATION 3

2.3 VULNERABILITY MANAGEMENT SYSTEM..... 3

2.3.1 VMS Systems..... 4

2.3.2 VMS Registration..... 4

2.3.3 VMS Tracked Assets..... 4

2.3.4 VMS Process Flow..... 4

2.4 COMPLIANCE STATUSES AND TIMEFRAMES 5

2.5 POA&M APPROVAL/REJECTION PROCESS 6

3 NECC CONFIGURATION CONTROL.....7

3.1 CONFIGURATION CONTROL ROLES AND RESPONSIBILITIES 7

3.1.1 Configuration Management Board..... 7

3.1.2 NECC Configuration Control Board..... 8

3.1.3 Engineering Review Board..... 8

3.1.4 Local CCB..... 9

3.2 NECC CONFIGURATION CONTROL PROCESS..... 9

3.2.1 NECC Change Request Process 10

4 NECC IAVM PROCESS.....10

4.1 NECC CAPABILITY MODULE IAVM PATCH PROCESS 10

4.1.1 IAVM Process Timeline 12

4.1.2 IAVM Process Involving a Significant Configuration Change 12

4.1.3 FDCE IAVM Process..... 13

4.1.4 NECC IAVM Roles and Responsibilities 13

5 POLICY/DIRECTIVES13

6 RELEVANT ASSOCIATED PROGRAM DOCUMENTS.....13

7 POINTS OF CONTACT14

APPENDIX A - ACRONYM LIST15

UNCLASSIFIED

LIST OF FIGURES

Figure 1: NECC Configuration Control Board Organization 8

LIST OF TABLES

Table 1: Timeframe Requirements for IAVM Notification..... 6

Table 2: NECC IAVM Process Timeline 12

UNCLASSIFIED

1 INTRODUCTION

Net-Enabled Command Capability (NECC) is the Department of Defense's (DoD's) principal program for Command and Control Capabilities (C2C) that will be accessible in a net-centric environment and will focus on providing the commander with the data and information needed to make timely, effective, and informed decisions. NECC draws from the Command and Control (C2) community to evolve current and provide new C2 capabilities into a fully integrated, interoperable, collaborative Joint solution. Warfighters can rapidly adapt to changing mission needs by defining and tailoring their information environment and drawing on capabilities that enable the efficient, timely, and effective command of forces and control of engagements.

The NECC Program will respond to the Warfighter's needs through disciplined development, test, and user engagement processes. NECC will provide capabilities which focus on Force Projection, Force Readiness, Situational Awareness, Intelligence, Force Employment (Air/Space Operations, Land Operations, Maritime/Littoral Operations), and Force Protection. The program's single, net-centric, services-based, C2 architecture will provide the decision support infrastructure that enables the Warfighter to access, display, and understand the information necessary to make efficient, timely, and effective decisions.

The NECC Information Assurance Vulnerability Management (IAVM) Plan provides top-level direction for coordinating/maintaining IAVM compliance with NECC's configuration management control process.

1.1 Objective

The objectives of the NECC IAVM Plan are to:

- Review the Defense Information Systems Agency (DISA) IAVM process with which NECC will comply.
- Review the NECC Configuration Management Plan (CMP).
- Present an NECC IAVM process that ties the IAVM process with NECC configuration management.

1.2 Scope

This document describes the NECC IAVM activities to be performed, and assigns responsibilities required to support the Joint Program Management Office (JPMO) and Component Program Management Office (CPMO) activities. It applies to Capability Modules (CMs) developed and maintained by the materiel providers as well as the Federated Development and Certification Environment (FDCE). It supports the System Development and Demonstration (SDD) phase of NECC to include the operational support for the Deployed Baselines. The SDD phase addresses the life cycle of the capability increments.

In this document, the application of IAVM to CMs implies application to constituent Capability Packages which include virtual machines, operating systems (OS), and ancillary software.

1.3 Reference Documents

[Net-Enabled Command Capability \(NECC\) Increment 1 System Development and Demonstration \(SDD\) Phase Configuration Management Plan, v1.0, July 27, 2007](#)¹

[DISA IAVM Process Handbook, v3.0, February 14, 2007](#)²

2 DISA IAVM PROCESS BACKGROUND³

As a DISA organization, NECC will follow the DISA IAVM process that conforms to Assistant Secretary of Defense for Networks and Information Integration (ASD(NII)) requirements.

2.1 DoD Vulnerability Notices

The IAVM process begins with the Joint Task Force-Global Network Operations (JTF-GNO)/Net-Defense monitoring relevant sources of information to discover security conditions that may require IAVM vulnerability notification. The JTF-GNO/Net-Defense will assess the vulnerability, risk, and potential operational impact and develop an IAVM notification. The JTF-GNO/Net-Defense will coordinate the potential IAVM vulnerability notification with (Combatant Commanders) COCOM/Service/Agencies (C/S/As), field activities, and DISA Field Security Operations (FSOs). If the results of the analysis indicate a need for action, the JTF-GNO/Net-Defense will approve and publish the IAVM vulnerability notification.

There are three types of vulnerability notifications.

1. **Information Assurance Vulnerability Alert (IAVA)** - An IAVA is generated when network vulnerability is severe, resulting in an immediate potentially severe threat to DoD systems and information. Due to the severity of the risk presented by these vulnerabilities, corrective action is of the highest priority. Upon receipt of IAVA vulnerability notices, C/S/As are required to acknowledge the IAVA within the timeframe specified by the JTF-GNO/Net-Defense in the vulnerability notice. IAVAs require immediate compliance. If compliance cannot be achieved, a Plan of Action & Milestones (POA&M), with acceptable mitigating controls, timelines, and completion dates, must be developed and approved by the Designated Accrediting Authority (DAA) or DAA Representative.
2. **Information Assurance Vulnerability Bulletin (IAVB)** - An IAVB addresses new vulnerabilities that do not pose an immediate risk to DoD systems, but are significant enough that noncompliance with the corrective action could escalate the risk. Although corrective action is recommended, but not required by DoD, NECC will perform the corrective action indicated by the IAVB. Each IAVB indicates an acknowledgement suspense date. If compliance cannot be achieved, a POA&M with acceptable mitigating controls, timelines,

¹ URL: <https://www.us.army.mil/suite/page/491726>

² DISA IAVM Process Handbook, v3.0, February 14, 2007, URL: <https://powhatan.iiiie.disa.mil/vulnerability-mgmt/documentation/index.html#handbook>

³ Ibid.

and completion dates must be developed and approved by the DAA or DAA Representative. Compliance timeframe requirements not specifically stated in the IAVB will comply with those listed in Section 2.4 based on the IAVB's severity code.

- 3. Technical Advisory (TA)** - A TA is generated when new vulnerabilities exist but are generally categorized as low risk. Potential escalation of these vulnerabilities is deemed unlikely, but the advisories are issued so that any risk of escalation in the future can be mitigated. TA vulnerability notices are for notification purposes only; no reporting is required. Although corrective action is recommended but not required by DoD, NECC will perform the corrective action indicated by the TA. Each TA indicates an acknowledgement suspense date. Compliance timeframe requirements not specifically stated in the TA will comply with those listed in Section 2.4 based on the TA's severity code.

Once the vulnerability notice has been developed, the JTF-GNO/Net-Defense notifies each C/S/A's point of contact, via approved communication channels, that an alert, bulletin, or technical advisory has been issued and that the details can be accessed at the JTF-GNO/Net-Defense Unclassified but Sensitive Internet Protocol Router Network (NIPRNet) website, <https://www.jtfgno.mil> or on the Secret Internet Protocol Router Network (SIPRNet) <https://www.jtfgno.smil.mil>.

2.2 NECC IAVM Implementation

NECC, as a DoD organization, is responsible for implementing IAVM guidance internally. To support the implementation of the IAVM process, the Vulnerability Compliance Tracking System (VCTS) feature of the Vulnerability Management System (VMS) is available at DISA installations to manage compliance information for each organization at the asset level. Compliance information is entered by organizations at the individual asset level via VCTS, summarized, and uploaded for visibility by the JTF-GNO/Net-Defense. This ensures that the statistics reported to the JTF-GNO/Net-Defense are current and that progress can be monitored on a regular basis.

2.3 Vulnerability Management System

The VMS DoD application is used to assist in managing its internal implementation of the IAVM process. VMS was developed as a means to comply with Chairman of the Joint Chiefs of Staff Instructions (CJSCI) 6510.01, Change 2, which requires each DoD C/S/A to develop a methodology for tracking compliance with the IAVM program. The VMS is designed to collect vulnerability and compliance information at the individual asset level.

Vulnerability compliance information for individual assets is maintained by the System Administrators (SAs) or Information Assurance Officers (IAOs). Program/Project/Enclave Managers, Information Assurance Managers (IAMs), and Organizational Oversight Users provide management and oversight. The DAAs or DAA Representatives perform monitoring of Programs/Project/Enclaves; approval/rejection of POA&M including Mitigation Plans; and adjudication of accreditation status.

VMS access is gained by filling out a System Authorization Access Request (SAAR) form (DD FORM 2875) and faxing it to the VMS Support Office. Permissions are granted by the JPMO IAM.

2.3.1 VMS Systems

There are two VMS systems: one for unclassified assets (NIPRNet), and one for classified assets (SIPRNet). All Information Technology (IT) assets that are susceptible to vulnerabilities shall be registered in the VMS.

2.3.2 VMS Registration

All IAVM information for *unclassified* assets will be registered in the *unclassified VMS* database. Information entered and stored in this database is considered Controlled Unclassified Information (CUI).

All IAVM information for *classified* assets will be registered in the *classified VMS* database. Information entered and stored into this database is considered no higher than Secret and must be protected accordingly. Since all NECC assets will be on the SIPRNet, they will be registered in the classified VMS database.

NECC CM assets will be registered in VMS during the Security Test and Evaluation (ST&E) for the CM's initial Certification and Accreditation (C&A). It is important to initiate the IAVM process as soon as possible after assets are registered in VMS to prevent IA vulnerability notification non-compliance from impacting C&A.

2.3.3 VMS Tracked Assets

Physical server(s) as well as virtual machines will be registered in VMS. Each asset, to include mirrored assets, must be registered in VMS. It is acknowledged there are mirrored installations. However, due to phased implementations and tendencies to change, it is required that each asset be registered accordingly.

2.3.4 VMS Process Flow

Once a vulnerability notice has been issued by the JTF-GNO/Net-Defense, the VMS will send notices via email over the command channels to the responsible individuals associated with the applicable assets. Notices will also be sent to all IAMs and organizational oversight users for all vulnerability notices issued. The VMS notice will direct the user to access the JTF-GNO/Net-Defense web page to obtain the detailed information for the specific vulnerability notice.

At least one SA or IAO for each asset must acknowledge receipt. That individual is then responsible for initiating the process of evaluating and correcting the vulnerability. The IAVM Receipt Acknowledgement function is also available to allow users with the IAM or Organization Update VMS permission to acknowledge on behalf of an organization.

As the status of the vulnerability changes, each asset in the VMS must be updated with the current status. For example, the status may indicate whether a fix was applied, a POA&M including a Mitigation Plan was requested, or that the vulnerability notice was not applicable to the component.

Further information regarding the IAVM process flow can be found in the user guide titled “VMS General Information” under the *Help Link* located at the top of the VMS web page.

2.4 Compliance Statuses and Timeframes

In VMS, an asset is registered with characteristics (i.e., OS, patch level, resident applications, etc.). These characteristics comprise the asset posture. The posture of the asset dictates the vulnerabilities associated with the asset. Every potential applicable vulnerability notice to an asset will be labeled with one of the following “Compliance Status” identifiers:

1. **Not Reviewed:** This status reflects a vulnerability that has the potential for escalation, but it is deemed unlikely or that the status has not been evaluated. DISA TAs default to this status.
2. **Not Applicable:** “Not Applicable” means the SA, IAO, IAM, or Program Manager (PM) has determined a recently released notice does not apply to the operational configuration of a registered asset in the VMS. The responsible user who made this decision is required to maintain all documentation to justify the “Not Applicable” status. The management hierarchy or the DAA/DAA Representative may request the documentation. Also, the documentation may be reviewed during the IAVM compliance validation process.
3. **Fixed/In Compliance:** This status means the SA, IAO, IAM, or PM has determined a registered asset is applicable to a recently released notice and is in compliance with the official patch or fix.
4. **Open:** This status means that the vulnerability notice impacts the asset; however, no protective actions have been put in place. An asset is assigned this status until the individual who has custody of the asset changes the status. DoD IAVAs and IAVBs will default to this status. Open vulnerabilities have sub-statuses for POA&M and Mitigation Plan processing.

Sub-statuses are as follows:

- **Open-POA&M Not Updated (ONU):** Vulnerability is “Open” and POA&M has not been submitted.
- **Open-POA&M within Days Allowed (OWD):** Vulnerability is “Open” and POA&M has been submitted within the days specified in the notice. Mitigation Plan is not required at this time.
- **Open-Mitigation Required-but not Provided (OMR):** Vulnerability is “Open” and POA&M, including a Mitigation Plan, is required but has not been provided.
- **Open-Mitigation Submitted (OMS):** Vulnerability is “Open” and POA&M, which includes a Mitigation Plan, has been submitted for DAA or DAA Representative approval.
- **Open-Mitigation Approved (OMA):** Vulnerability is “Open” and POA&M, which includes a Mitigation Plan, has been approved by the DAA or DAA Representative.

The compliance timelines for IAVAs are in effect upon issuance, and they are mandatory as directed by the JTF-GNO/Net-Defense. The timeline for compliance on IAVBs and TAs

vulnerabilities are determined by the assigned severity for the vulnerability coupled with the compliance timelines listed below.

Severity codes (“[Security Technical Implementation Guide(s)] STIG Finding Severity”) are documented in the IAVM notices published on the JTF-GNO/Net-Defense web page. NECC will comply with the following timeframe requirements based on severity if the compliance/mitigation date is not specified in the IAVM notification.

Table 1: Timeframe Requirements for IAVM Notification

Severity	Days for Compliance/Approved Mitigation
CAT I	Immediate – 25 Days
CAT II	60 Days
CAT III	180 Days
CAT IV	1000 Days

2.5 POA&M Approval/Rejection Process

Once a POA&M with a Mitigation Plan has been initiated, it is forwarded to the IAM for approval or rejection. If approved, the POA&M is forwarded to the DAA or DAA Representative for approval or rejection. POA&M guidance is provided in the DISA IAVM Process Handbook.

- If **approved** by the DAA or DAA Representative, the status of the asset is changed to “Open-Mitigation Approved”. The Scheduled Completion Date field is updated, if necessary, to indicate the date that full compliance is expected to be achieved. The DAA or DAA Representative may also provide text that needs to be reviewed by the SA. Additionally, an e-mail is sent to the submitter of the POA&M indicating the approval. At this point, the SA/IAO has until the estimated completion date associated with the vulnerability notice to come into compliance. Management is responsible for continuing to address the problem and ensure that mitigating controls are in place.
- If **rejected** by the DAA or DAA Representative, comments explaining the reason for the rejection are provided. Additionally, an e-mail is sent to the submitter of the POA&M indicating the rejection. At this point, it becomes the responsibility of the SA/IAO to correct the vulnerability associated with the asset and to comply with any comments provided by the DAA or DAA Representative.

3 NECC CONFIGURATION CONTROL⁴

Configuration control is the establishment of orderly and effective procedures for processing all changes to affected NECC Critical Configuration Items (CCIs) and baseline configuration documentation. Configuration control is required to ensure systematic submission, coordination, evaluation, selection, and release of approved changes to the established NECC Baselines. Change Requests (CRs) to the NECC Technical Baseline can be initiated by NECC users, developers, test, and evaluation teams; NECC engineering activities; Help Desk processes; IA vulnerability management; or as a result of Capabilities Provisioning Activities (CPAS). Configuration control shall be established and implemented throughout the NECC life cycle to ensure that only properly evaluated and approved changes are incorporated and that NECC compliance and change accountability is maintained.

This element of configuration management identifies the groups participating in the processes, provides for baseline management, and promotes interface control. Once the CCIs are established, baseline management is achieved through the application of the formal change process. During NECC evolution, configuration control will facilitate the rapid, agile integration and transition of existing applications, and the sharing of the NECC infrastructure and enabling services. Configuration management encompasses the formal change control process that enables conflict resolution, interface management, and program optimization.

3.1 Configuration Control Roles and Responsibilities

The JPMO Configuration Management organization, described in the following paragraphs, is responsible for maintaining configuration control over the CCI developmental configurations and baselines, and for processing changes to those CCIs. This is accomplished by administering the processes of version control, change control, reporting, and auditing. The Configuration Management organization implements these processes to ensure that products developed are correct, consistent, complete, and compliant with governing policies.

The NECC Configuration Management Board (CMB) is the governing body that sets configuration management objectives and priorities, and oversees CCI development and deployment activities. The NECC Configuration Control Board (CCB) is the primary means of establishing and maintaining the integrity of the products of the NECC throughout the program's life cycle.

3.1.1 Configuration Management Board

The NECC CMB is the configuration management governing body and the senior forum for adjudicating issues referred by the CCB concerning development, content, and scheduling of NECC CM baseline releases. As the most senior program configuration control authority, the CMB typically only reviews CRs forwarded by the NECC CCB for decision that are beyond the developers' NECC scope or funding negotiated through a Service Level Agreement (SLA). The

⁴ Derived from Net-Enabled Command Capability (NECC) Increment 1 System Development and Demonstration (SDD) Phase Configuration Management Plan, v1.0, July 27, 2007

CMB will refer those that exceed pre-established thresholds to the Joint Program Executive Office (JPEO) C2C for decision.

3.1.2 NECC Configuration Control Board

The NECC CCB will establish and approve the Technical Baseline, maintain and manage formal configuration control over established baselines, ensure CRs are sufficiently assessed for scope and impact, and disposed of and approve changes incorporated into NECC baselines. The CCB is the responsible authority for approval of recommended changes to all CMs.

The NECC CCB uses an Engineering Review Board (ERB) to conduct a technical review and assessment of certain change requests before determining their disposition. The ERB will elicit help from and coordinate with the appropriate Subject Matter Experts (SME) as appropriate.

Proposed changes deemed beyond the scope of the NECC CCB or requiring significant fiscal commitments are forwarded to the CMB for approval/disapproval. The CMB will refer those changes that exceed pre-established thresholds to the JPEO for decision.

The NECC CCB membership includes representatives from the NECC JPMO, United States Joint Forces Command (USJFCOM), and each CPMO as depicted below in Figure 1.

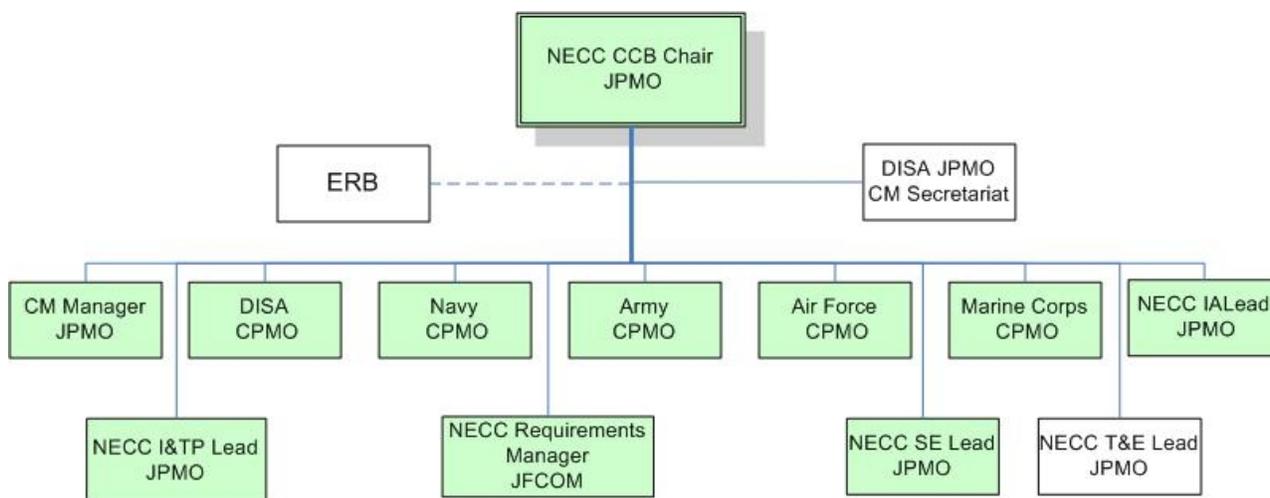


Figure 1: NECC Configuration Control Board Organization

3.1.3 Engineering Review Board

At the direction of the NECC CCB, the ERB conducts an analysis of proposed CRs to identify critical configuration items affected by the changes and works with the appropriate CPMO to determine the costs, impacts, and benefits associated with proposed CR.

ERB members speak for the JPMO and CPMO they represent and are expected to articulate the technical position of that CPMO in meeting discussions and decisions. These members serve as technical advisors to the NECC CCB.

3.1.4 Local CCB

The Local CCB shall have cognizance over the individual CMs' internal baselines. The Local CCB is responsible for assessing proposed changes and known problems reported against the materiel solution (i.e., CM), adjudicating change requests, and maintaining configuration control of the CMs assigned to them as the materiel provider. The Local CCB is responsible for approving code changes that affect version numbers at the third or fourth digit. Changes that affect the first and second digit of a CM's version or changes that may affect the interface must be approved at the NECC CCB. This Local CCB will provide detailed information and recommendations on issues that must be elevated to the NECC CCB level.

3.2 NECC Configuration Control Process

The purpose of the Configuration Control Process is to initiate, monitor, and facilitate implementation changes that cross systems or processes between functional communities. These changes across systems or processes are referred to as NECC CRs. The goals of the Change Control Process are to:

- a. Manage, implement, and effectively track the NECC CRs
- b. Provide a method for the initiator to ascertain the status of a CR
- c. Ensure feedback to the appropriate authority for model updates (e.g., data and network)
- d. Identify duplicate activities across systems and functions
- e. Identify common data elements across systems
- f. Identify and establish new CCIs
- g. Ensure communication among CR initiators, coordinators, and reviewers
- h. Monitor the status of a CR and feedback to end-users
- i. Provide open communications to raise issues associated with CRs
- j. Ensure a streamlined method for conflict resolution
- k. Provide a method to measure the success of the process
- l. Enable continuous process improvement based on the measures or metrics
- m. Identify training requirements
- n. Facilitate operational assessment of the change in capability.

3.2.1 NECC Change Request Process

Details of the NECC Change Request Process can be found in the [Net-Enabled Command Capability Increment 1 System Development and Demonstration \(SDD\) Phase Configuration Management Plan \(CMP\)](#).⁵

4 NECC IAVM PROCESS

4.1 NECC Capability Module IAVM Patch Process

The NECC IAVM process provides a means to obtaining positive control down to the system asset level. The process streamlines the change control process specifically for IAVM notifications with the highest level of urgency, as mandated by the JTF-GNO.

A CM will consist of one or more Capability Packages (CPs) tailored to the type of deployment environment (e.g., enterprise or local). The services provided by a CM are instantiated through CPs. A CP consists of four kinds of software: a virtual machine, a guest OS, an operational set of supporting Commercial-Off-The-Shelf (COTS) infrastructure software such as a web server, and NECC-developed (or adopted) software. The IAVM process will be applied to the CP components.

In addition to meeting the JTF-GNO IAVM requirements, the NECC IAVM process will conform to the CR and CCB processes. The CR and CCB processes will be defined in the CMP.

IAVM testing will be performed in the FDCE. The FDCE is a federated development, integration, testing, and certification environment, which will be established by DISA, the Services, and COCOMs.

1. JTF-GNO Issues an IAVM Notification. The NECC CPMO IA will review all IAVM Notifications and acknowledge the receipt of IAVA or IAVB via VMS. The hosting site (e.g., Defense Enterprise Computer Center (DECC)) will also review IAVM notifications and await implementation approval and instructions. **Suspense: Day 0, CPMO IA Acknowledges IAVM.**
2. The NECC CPMO IA will consult with CM developers/integrators to assess the IAVM Notification's applicability to their respective NECC CM baseline and whether the IAVM will affect the CM baseline. If the IAVM Notification is determined to be "Not Applicable", the NECC CPMO IA will ensure VMS is updated accordingly, and no additional action is required. If the IAVM notification is determined to be applicable, the CPMO IA along with developers/integrators will estimate the time to install the IAVM fix. NECC CPMO IA generates a CR and forwards it to the CPMO Local CCB. If the IAVM affects the CM baseline, the Local CCB will have to determine a course of action and whether the process described in Section 4.1.1 will have to be followed. **Suspense: Day 1, CPMO IA Generates CR**

⁵ Increment 1 System Development and Demonstration (SDD) Phase Configuration Management Plan, v1.0, 27 July 2007, URL: <https://www.us.army.mil/suite/page/491726>

UNCLASSIFIED

3. The NECC CPMO IA, with input from developers/integrators, will determine whether the fix can be tested and installed within the IAVM compliance date. If not, the NECC CPMO IA will generate a VMS POA&M which includes a Mitigation Plan and schedule. If the fix can be installed by the compliance date, it is installed on the CM in the appropriate FDCE environment and tested. For example, if the CM is either in the development, developmental piloting, or operational prototyping environment stage, it will be tested in its respective environment. However, if the CM is operational, it will be installed in the operational prototyping environment. The NECC CPMO IA will update the IAVM status in VMS. Once installed, the materiel developer will perform regression testing, analysis of new issues, performance impact testing, etc. Results are recorded and recommendation generated. The IAV fix test results and recommendation are presented to the CPMO Local CCB. **Suspense, Day 6, CPMO IA Provides Test Results to CPMO Local CCB.**
4. The CPMO Local CCB will review the results and either approve or disapprove the IAVM fix. The NECC JPMO CCB will be notified on all IAVM decisions. In situations where waiting for the next scheduled CPMO Local CCB meeting poses an unacceptable delay in the process, NECC CPMO IA shall request an emergency CCB decision by email. The NECC JPMO CCB is copied on all IAVM CRs. **Suspense: Day 11, CCB Makes Decision on IAVM Fix Installation.**
 - a. If the IAVM fix causes an operational impact and is disapproved for installation, then:
 - The CPMO Local CCB will work with the materiel developer to correct issues to prevent operation impact.
 - The NECC CPMO IA will, if necessary, update or generate the POA&M, which includes a Mitigation Plan and schedule.
 - IAV fix will be uninstalled from the CM.
 - Go to step 6.
 - b. If the IAV fix causes no operational impact and is approved, then:
 - NECC CPMO IA and the materiel developer will coordinate to incorporate IAVM fix installation procedures in the appropriate NECC CM installation procedures.
 - NECC JPMO CCB will update the build list and update CM implementation baseline.
 - The closure of the IAVM is recorded in VMS.
 - If CM is an operational CM:
 - The CPMO will be responsible for having the fix installed. (**Suspense: Day 12, CPMO has IAVM fix installed**). Installation is per recommended procedure during a CCB coordinated maintenance period.
 - The Tier 3 Service Desk will be informed of the IAV fix installation.
5. NECC CPMO IA generates or updates POA&M as necessary. **Suspense: 5 Days Prior to POA&M Mitigation Date, the CPMO IA generates or updates POA&M as necessary**
6. DAA approves/disapproves POA&M. **Suspense: POA&M Mitigation Date.**

4.1.1 IAVM Process Timeline

The table below represents the timeline that will be followed for the NECC IAVM process.

Table 2: NECC IAVM Process Timeline

Day	Process Step	Suspense (Required by Timeline)
0	1	CPMO IA acknowledges IAVM
1	2	CPMO IA generates CR
6	3	CPMO IA provides test results to CPMO Local CCB
11	4	LCCB either authorizes or doesn't authorize IAVM fix installation
12	4.2	CPMO has IAVM fix installed
5 days prior to Mitigation date	5	CPMO IA generates or updates POA&M as necessary
Mitigation date	6	DAA approves/disapproves POA&M

The Mitigation date is the date by which assets must be brought in compliance with the IA vulnerability notice or a POA&M must be approved. If the Mitigation date is not listed in the IA vulnerability notice, it is based on the timelines listed in Section 2.4.

4.1.2 IAVM Process Involving a Significant Configuration Change

The above procedure is appropriate for a typical IAV patch. However, there is the possibility that the IAVM Notification (IAVA, IAVB, or TA) may prescribe more extensive changes. For example, the IAVM notification may require the recoding of a Government-Off-The-Shelf (GOTS) component or an update or replacement of a COTS component. These changes would affect the version numbers at the first or second digit, and since the Local CCBs are only responsible for changes that affect version numbers at the third for fourth digit, the CPMO Local CCB will forward the CR to the JPMO CCB and ERB for review. The JPMO ERB will work with the CPMO Local CCB and respective materiel developer to make the required changes. Once the changes have been developed and tested, a Change Notification citing the changes will be sent to the Certifier (e.g., FSO) for approval and then the DAA for approval. Depending on the extent of the required change, the Certifier and/or DAA may recommend a ST&E be performed prior to approval and subsequent installation. In addition, the version number will be updated accordingly. Finally, since the changes are unlikely to be completed by the Mitigation date, the CPMO IA will be required to generate a POA&M and have it approved by the DAA.

4.1.3 FDCE IAVM Process

With respect to the FDCE, the IAVM process will be exactly the same as described in Section 4.1 with the exceptions that it will be handled entirely within the NECC JPMO as opposed to the CPMO, and the FDCE CCB will replace the CPMO Local CCB.

4.1.4 NECC IAVM Roles and Responsibilities

The following bullets review the general roles and responsibilities:

- United States Strategic Command (USSTRATCOM) DAA: IAVM compliance monitoring via VMS, POA&M approval.
- JPMO: IAVM compliance monitoring via VMS, JPMO CCB, and ERB functions.
- CPMO: IAV notice acknowledgement and compliance updating, POA&M generation, Local CCB & Local ERB functions, CR generation, regression testing, and IAV notice implementation

5 POLICY/DIRECTIVES

- Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01E, *Joint Capabilities Integration and Development System*, 11 May 2005
- CJCSI 6211.02B, *Defense Information System Network (DISN): Policy, Responsibilities and Processes*, 31 July 2003
- CJCSI 6212.01D, *Interoperability and Supportability of National Security Systems (NSS) and Information Technology (IT) Systems*, 8 Mar 06
- CJCSI 6510.01D, *Information Assurance (IA) and Computer Network Defense (CND)*, 15 Jun 04
- Department of Defense Directive (DoDD) 4630.5, *Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)*, 5 May 04
- DoDD 8500.1, *Information Assurance*, 24 Oct 02
- Department of Defense Instruction (DoDI) 4630.8, *Procedures for Interoperability and Supportability of IT and NSS*, 30 Jun 04
- DoDI 8500.2, *Information Assurance Implementation*, 6 February 03
- DoDI 8520.2, *Public Key Infrastructure (PKI) and Public Key Enabling (PKE)*, 1 Apr 04
- DoDI 8580.1, *Information Assurance (IA) in the Defense Acquisition System*, 9 Jul 04
- 10 U.S.C. Section 2224, *Defense Information Assurance Program*, 18 Mar 04

6 RELEVANT ASSOCIATED PROGRAM DOCUMENTS

This NECC IAVM Plan version reflects these capabilities and program documents:

UNCLASSIFIED

Net-Enabled Command Capability (NECC) Increment 1 System Development and Demonstration (SDD) Phase Configuration Management Plan (CMP), v1.0, July 27, 2007

7 POINTS OF CONTACT

The NECC program is managed by the Defense Information Systems Agency, P.O. Box 4502, Arlington, VA 22204-4502.

**PROGRAM MANAGER /
DISA-NECC**

Laura Knight
Program Manager
Laura.Knight@disa.mil
703 882-2268

**BRANCH CHIEF/
NECC PROGRAM CONTROL**

Kimberly Davis
Chief, Program Control
Kimberly.Davis@disa.mil
703 882-1269

**IA MANAGER /
NECC-CC12**

Steve Koehler, DISA
NECC Information Assurance
Steve.Koehler@disa.mil
703 882-0297

APPENDIX A - ACRONYM LIST

Acronym	Definition
ASD(NII)	Assistant Secretary of Defense for Networks and Information Integration
C&A	Certification and Accreditation
C/S/A	Combatant Commanders/Services/Agencies
C2	Command and Control
C2C	Command and Control Capabilities
CAT	Category
CCB	Configuration Control Board
CCI	Critical Configuration Item
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CM	Capability Modules
CMB	Configuration Management Board
CMP	Configuration Management Plan
CND	Computer Network Defense
COCOM	Combatant Command
COTS	Commercial-Off-The-Shelf
CPAS	Capability Provisioning Activities
CPMO	Component Program Management Office
CR	Change Request
DAA	Designated Accrediting Authority
DECC	Defense Enterprise Computing Center
DISA	Defense Information Systems Agency
DISA COI	DISA Chief Information Officer
DISN	Defense Information System Network
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
ERB	Engineering Review Board
FDCE	Federated Development and Certification Environment
FSO	Field Security Operations
GOTS	Government-Off-The-Shelf

UNCLASSIFIED

Acronym	Definition
IA	Information Assurance
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IAVA	Information Assurance Vulnerability Alert
IAVB	Information Assurance Vulnerability Bulletin
IT	Information Technology
JPEO	Joint Program Executive Office
JPMO	Joint Program Management Office
JTF-GNO	Joint Task Force-Global network Operations
NECC	Net-Enabled Command Capability
NIPRNet	Non-secure Internet Protocol Router Network
NSS	National Security Systems
OMA	Open-Mitigation Approved
OMR	Open-Mitigation Required
OMS	Open-Mitigation Submitted
ONU	Open-POA&M Not Updated
OS	Operating System
OWD	Open-POA&M within Days (Allowed)
PKE	Public Key Encryption
PKI	Public Key Infrastructure
PM	Program Manager
POA&M	Plan of Action and Milestones
SA	System Administrator
SAAR	System Authorization Access Request
SDD	System Development and Demonstration
SIPRNet	Secret Internet Protocol Router Network
SLA	Service Level Agreements
SME	Subject Matter Expert
ST&E	Security Test and Evaluation
STIG	Security Technical Implementation Guide
TA	Technical Advisory
U.S.C	United States Code
USJFCOM	US Joint Forces Command

UNCLASSIFIED

Acronym	Definition
USSTRATCOM	United States Strategic Command
VCTS	Vulnerability Compliance Tracking System
VMS	Vulnerability Management System